

Docket No.: 65933-083

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of _____ : Customer Number: 20277

Yoshihiro HORI, et al. : Confirmation Number:

Serial No.: : Group Art Unit:

Filed: March 26, 2004 : Examiner:

For: METHOD AND APPARATUS FOR ENCRYPTING DATA TO BE SECURED AND
INPUTTING/OUTPUTTING THE SAME

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

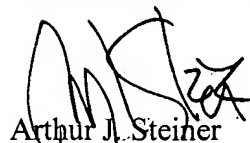
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-092946, filed March 28, 2003

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Arthur J. Steiner
Registration No. 26,106

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 AJS:prg
Facsimile: (202) 756-8087
Date: March 26, 2004

WDC99 898606-1.065933.0083



日 本 国 特 許 庁
JAPAN PATENT OFFICE

65933-083
Hori et al.
March 26, 2004
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 3 月 2 8 日

出 願 番 号
Application Number: 特 願 2 0 0 3 - 0 9 2 9 4 6

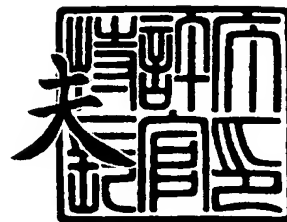
[ST. 10/C]: [J P 2 0 0 3 - 0 9 2 9 4 6]

出 願 人
Applicant(s): 三洋電機株式会社
シャープ株式会社
日本ビクター株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社

2 0 0 4 年 1 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 NQC1020098

【提出日】 平成15年 3月28日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 19/00

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 堀 吉宏

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 金井 雄一

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 大野 良治

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株式会社内

【氏名】 大石 剛士

【発明者】

【住所又は居所】 埼玉県所沢市花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内

【氏名】 多田 謙一郎

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 平井 達哉

【発明者】

【住所又は居所】 東京都千代田区丸の内 1 丁目 3 番地 1 号 東京銀行協会
ビル 1 4 F フェニックステクノロジーズ株式会社内

【氏名】 津留 雅文

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 長谷部 高行

【特許出願人】

【識別番号】 000001889

【氏名又は名称】 三洋電機株式会社

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 300017636

【氏名又は名称】 フェニックステクノロジーズ株式会社

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100105924

【弁理士】

【氏名又は名称】 森下 賢樹

【電話番号】 03-3461-3687

【手数料の表示】

【予納台帳番号】 091329

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ入出力方法、およびその方法を利用可能な記憶装置およびホスト装置

【特許請求の範囲】

【請求項 1】 データを保持する記憶媒体と、

前記記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数行う際に、該複数の暗号入出力処理をそれぞれ複数の手順に分割して発行された複数の命令を前記ホスト装置から受信し、該命令を実行する暗号処理部と、を備え、

前記暗号処理部は、前記命令に付された識別情報を参照して、受信した命令がいずれの暗号入出力処理に属する命令であることを識別し、前記複数の暗号入出力処理手順のうちの 2 以上の処理を並行して処理可能であることを特徴とする記憶装置。

【請求項 2】 前記暗号処理部は、前記暗号入出力処理ごとに、前記命令の実行順序を管理し、順序の不正な命令を受信したときに、該命令の実行を拒否することを特徴とする請求項 1 に記載の記憶装置。

【請求項 3】 前記暗号処理部は、順序の不正な命令を受信したときに、該命令が属する暗号入出力処理を中止することを特徴とする請求項 2 に記載の記憶装置。

【請求項 4】 前記記憶装置が並行して処理可能な暗号入出力処理の数は、前記記憶装置の性能に基づいて予め決定されることを特徴とする請求項 1 から 3 のいずれかに記載の記憶装置。

【請求項 5】 前記ホスト装置からの要求に応じて、前記記憶装置が並行して処理可能な暗号入出力処理の最大数を前記ホスト装置に提供することを特徴とする請求項 1 から 4 のいずれかに記載の記憶装置。

【請求項 6】 前記記憶媒体は、通常のデータを保持する通常データ記憶部と、前記秘匿すべきデータを保持する機密データ記憶部と、を含み、

前記機密データ記憶部は、前記暗号処理部を介してのみアクセス可能に構成されることを特徴とする請求項 1 から 5 のいずれかに記載の記憶装置。

【請求項 7】 データを保持する記憶媒体と、

前記記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を行う際に、該暗号入出力処理を複数の手順に分割して発行された複数の命令を前記ホスト装置から受信し、該命令を実行する暗号処理部と、を備え、

前記暗号処理部は、2 以上の暗号入出力処理を管理可能であり、命令に付された識別情報を参照して、受信した命令がいずれの暗号入出力処理に属する命令であるかを識別し、該命令が属する暗号入出力処理において不正な順序の命令であることを検知したとき、該命令の実行を拒否することを特徴とする記憶装置。

【請求項 8】 前記ホスト装置からの要求に応じて、前記記憶装置が並行して処理可能な暗号入出力処理の最大数を前記ホスト装置に提供することを特徴とする請求項 7 に記載の記憶装置。

【請求項 9】 秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数並行して処理可能に構成された記憶装置との間でデータを入出力するホスト装置であって、

前記暗号入出力処理を複数の手順に分割し、それらの手順のうち前記記憶装置側で実行すべき手順を前記記憶装置に実行させるための命令を前記記憶装置に対して順に発行するコントローラと、

前記暗号入出力処理に必要な暗号化または復号処理を実行する暗号処理部と、を備え、

前記コントローラは、前記命令を発行するときに、該命令が、前記複数の暗号入出力処理のうちいずれの暗号入出力処理に属する命令であるかを識別するための識別情報を、該命令に付すことを特徴とするホスト装置。

【請求項 10】 前記コントローラは、前記暗号入出力処理の開始に先立って、該暗号入出力処理を行う処理系を確保するための命令を発行することを特徴とする請求項 9 に記載のホスト装置。

【請求項 11】 秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数並行して実行可能に構成され、かつ、前記暗号入出力処理によって入出力するデータを保持する記憶装置とホスト装置との間で、前記暗号入

出力処理を実行する際に、

前記暗号入出力処理を複数の手順に分割し、それらの手順のうち前記ホスト装置側で実行すべき手順を前記ホスト装置が実行するステップと、

前記記憶装置側で実行すべき手順を前記記憶装置に実行させるために、前記ホスト装置が前記記憶装置に対して命令を発行するステップと、

前記記憶装置が前記命令を受信するステップと、

前記記憶装置が前記命令を実行するステップと、を含み、

前記命令には、該命令が、前記記憶装置が並行して処理している複数の暗号入出力処理のうちいずれの暗号入出力処理に属する命令であるかを識別するための識別情報が付されることを特徴とするデータ入出力方法。

【請求項 12】 前記記憶装置の性能に基づいて、前記記憶装置が並行して処理可能な前記暗号入出力処理の数の上限を予め決定するステップをさらに含むことを特徴とする請求項 11 に記載のデータ入出力方法。

【請求項 13】 前記記憶装置が、自身の性能に基づいて、並行して処理可能な前記暗号入出力処理の数の上限を予め決定するステップと、

前記上限を前記ホスト装置に通知するステップと、

をさらに含むことを特徴とする請求項 11 に記載のデータ入出力方法。

【請求項 14】 前記暗号入出力処理の実行に先立って、前記決定するステップで決定した数だけ用意された前記識別情報の中から、実行しようとする暗号入出力処理を識別するための識別情報を選択して割り当てるステップをさらに含むことを特徴とする請求項 12 または 13 に記載のデータ入出力方法。

【請求項 15】 前記受信するステップは、

受信した命令が、前記暗号入出力処理において正しい実行順序の命令であるかを判別するステップと、

正しい実行順序の命令であると判別されたときに、該命令を正常に受理するステップと、

不正な実行順序の命令であると判別されたときに、該命令の実行を拒否するステップと、

を含むことを特徴とする請求項 11 から 14 のいずれかに記載のデータ入出力

方法。

【請求項 1 6】 受信した命令が不正な実行順序の命令であると判別されたときに、その命令が属する暗号入出力処理の実行を中止することを特徴とする請求項 1 5 に記載のデータ入出力方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データ入出力技術に関し、とくに、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力する技術に関する。

【 0 0 0 2 】

【従来の技術】

近年、記憶素子の小型化、集積化、量産化が飛躍的に進み、記録媒体の小型化、大容量化、低価格化が進んでいる。そのような状況下、本出願人らは、さらに利便性の高い記録媒体の実現を目指し、従来一つのホスト装置に固定的に接続されて使用されるのが一般的であった大容量ハードディスクを、ホスト装置に着脱自在に構成することにより、複数のホスト装置でデータを共有可能なリムーバブルメディアとして扱えるようにしようと考えた。小型かつ大容量で、アクセス速度も比較的高速なハードディスクをリムーバブルメディアとして利用できることのメリットは大きい。

【 0 0 0 3 】

【特許文献 1】

特開 2 0 0 0 - 1 7 3 1 5 8 号公報 (全文)

【 0 0 0 4 】

【発明が解決しようとする課題】

ユーザの利便性を考えると、あらゆるホスト装置でこのリムーバブルなハードディスクを読み書きできるようにすることが望ましいが、反面、あらゆるホスト装置で読み書き可能ということは、第三者にデータが漏洩する危険性もはらんでいることを意味する。音楽や映像などのデジタルコンテンツの流通が注目される現在、著作権を保護し、デジタルコンテンツの流出を防ぐためにも、秘匿すべき

データを適切に保護することのできる技術を開発することが重要である。

【0005】

本発明はこうした状況に鑑みてなされたものであり、その目的は、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するときの耐タンパ性を向上させる技術の提供にある。本発明の別の目的は、記憶装置とホスト装置との間で実行される暗号化入出力処理の効率を向上させる技術の提供にある。

【0006】

【課題を解決するための手段】

本発明のある態様は、記憶装置に関する。この記憶装置は、データを保持する記憶媒体と、記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数行う際に、該複数の暗号入出力処理をそれぞれ複数の手順に分割して発行された複数の命令をホスト装置から受信し、該命令を実行する暗号処理部と、を備え、暗号処理部は、命令に付された識別情報を参照して、いずれの暗号入出力処理に属する命令であるかを識別し、複数の暗号入出力処理手順のうちの2以上の処理を並行して処理可能である。

【0007】

後述するように、暗号入出力処理を複数の手順に分割し、命令を細分化することで、バスを効率良く開放し、複数の処理を並列に実行させることが可能となる。このとき、複数の処理に属する命令が並列して発行されるので、それらを適切に識別するために、命令に識別情報を付す。

【0008】

暗号処理部は、暗号入出力処理ごとに、命令の実行順序を管理し、順序の不正な命令を受信したときに、該命令の実行を拒否してもよい。暗号処理部は、順序の不正な命令を受信したときに、該命令が属する暗号入出力処理を中止してもよい。暗号入出力処理における命令の実行手順を入れ替えるとセキュリティホールが生じる恐れがあるが、実行順序を適切に管理することにより、不正アクセスを防ぐことができる。

【0009】

記憶装置が並行して処理可能な暗号入出力処理の数は、記憶装置の性能に基づ

いて予め決定されてもよい。記憶装置は、ホスト装置からの要求に応じて、記憶装置が並行して処理可能な暗号入出力処理の最大数をホスト装置に提供してもよい。これにより、記憶装置の性能に応じて適切な数の処理系を用意することができる。記憶媒体は、通常データを保持する通常データ記憶部と、秘匿すべきデータを保持する機密データ記憶部と、を含み、機密データ記憶部は、暗号処理部を介してのみアクセス可能に構成されてもよい。これにより、秘匿すべきデータが漏洩する危険性を最小限に抑えることができる。

【 0 0 1 0 】

本発明の別の態様も、記憶装置に関する。この記憶装置は、データを保持する記憶媒体と、記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を行う際に、該暗号入出力処理を複数の手順に分割して発行された複数の命令をホスト装置から受信し、該命令を実行する暗号処理部と、を備え、暗号処理部は、2以上の暗号入出力処理を管理可能であり、命令に付された識別情報を参照して、受信した命令がいずれの暗号入出力処理に属する命令であることを識別し、該命令が属する暗号入出力処理において不正な順序の命令であることを検知したとき、該命令の実行を拒否する。

【 0 0 1 1 】

この記憶装置は、ホスト装置からの要求に応じて、記憶装置が並行して処理可能な暗号入出力処理の最大数を前記ホスト装置に提供してもよい。

【 0 0 1 2 】

本発明のさらに別の態様は、ホスト装置に関する。このホスト装置は、匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数並行して処理可能に構成された記憶装置との間でデータを入出力するホスト装置であって、暗号入出力処理を複数の手順に分割し、それらの手順のうち記憶装置側で実行すべき手順を記憶装置に実行させるための命令を記憶装置に対して順に発行するコントローラと、暗号入出力処理に必要な暗号化または復号処理を実行する暗号処理部と、を備え、コントローラは、命令を発行するときに、該命令が、複数の暗号入出力処理のうちいずれの暗号入出力処理に属する命令であることを識別するための識別情報を、該命令に付す。

【0013】

コントローラは、暗号入出力処理の開始に先立って、該暗号入出力処理を行う処理系を確保するための命令を発行してもよい。この命令は、該暗号入出力処理を識別するための識別情報を確保する処理であってもよい。

【0014】

本発明のさらに別の態様は、データ入出力方法に関する。この方法は、秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数並行して実行可能に構成され、かつ、暗号入出力処理によって入出力するデータを保持する記憶装置とホスト装置との間で、暗号入出力処理を実行する際に、暗号入出力処理を複数の手順に分割し、それらの手順のうちホスト装置側で実行すべき手順をホスト装置が実行するステップと、記憶装置側で実行すべき手順を記憶装置に実行させるために、ホスト装置が記憶装置に対して命令を発行するステップと、記憶装置が命令を受信するステップと、記憶装置が命令を実行するステップと、を含み、命令には、該命令が、記憶装置が並行して処理している複数の暗号入出力処理のうちいずれの暗号入出力処理に属する命令であるかを識別するための識別情報が付される。

【0015】

この方法は、記憶装置の性能に基づいて、記憶装置が並行して処理可能な暗号入出力処理の数の上限を予め決定するステップをさらに含んでもよい。この方法は、記憶装置が、自身の性能に基づいて、並行して処理可能な暗号入出力処理の数の上限を予め決定するステップと、上限をホスト装置に通知するステップと、をさらに含んでもよい。暗号入出力処理の実行に先立って、決定するステップで決定した数だけ用意された識別情報の中から、実行しようとする暗号入出力処理を識別するための識別情報を選択して割り当てるステップをさらに含んでもよい。

【0016】

受信するステップは、受信した命令が、暗号入出力処理において正しい実行順序の命令であるか否かを判別するステップと、正しい実行順序の命令であると判別されたときに、該命令を正常に受理するステップと、不正な実行順序の命令で

あると判別されたときに、該命令の実行を拒否するステップと、を含んでもよい。受信した命令が不正な実行順序の命令であると判別されたときに、その命令が属する暗号入出力処理の実行を中止してもよい。

【 0 0 1 7 】

なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【 0 0 1 8 】

【発明の実施の形態】

(第 1 の実施の形態)

図 1 は、第 1 の実施の形態に係るデータ管理システム 1 0 の全体構成を示す。データ管理システム 1 0 は、ストレージデバイス 2 0 0 へのデータの記録を制御する記録装置 1 0 0、ストレージデバイス 2 0 0 に記録されたデータの再生を制御する再生装置 3 0 0、およびデータを記憶保持するストレージデバイス 2 0 0 を備える。本実施の形態のストレージデバイス 2 0 0 は、データを保持する記憶媒体だけでなく、記録装置 1 0 0 または再生装置 3 0 0 などのホスト装置と記憶媒体との間でのデータの入出力を制御するコントローラなどの構成を備えるドライブ一体型の記憶装置である。本実施の形態では、ストレージデバイス 2 0 0 として、ハードディスクドライブを例にとって説明する。

【 0 0 1 9 】

従来のハードディスクは、一つのホスト装置に固定的に接続されて使用されるのが一般的であったが、本実施の形態のストレージデバイス 2 0 0 は、記録装置 1 0 0 および再生装置 3 0 0 などのホスト装置に対して着脱自在に構成されている。すなわち、本実施の形態のストレージデバイス 2 0 0 は、CD や DVD などと同様にホスト装置から取り外して持ち運ぶことができ、記録装置 1 0 0、再生装置 3 0 0、記録および再生が可能な記録再生装置など、複数のホスト装置間で共用することが可能な記憶装置である。

【 0 0 2 0 】

このように、本実施の形態のストレージデバイス 2 0 0 は、複数のホスト装置

に接続されることを前提にしており、たとえば所有者以外の第三者のホスト装置に接続されて、内部に記録されたデータを読み出される可能性もある。このストレージデバイス 2 0 0 に、音楽や映像などの著作権により保護されるべきコンテンツ、企業や個人の機密情報などの秘匿すべきデータを記録することを想定したとき、それらの秘匿データが外部に漏洩することを防ぐためには、ストレージデバイス 2 0 0 自身にデータを適切に保護するための構成を設け、十分な耐タンパ機能を持たせることが好ましい。このような観点から、本実施の形態のストレージデバイス 2 0 0 は、ホスト装置との間で秘匿データを入出力するときに、その秘匿データを暗号化してやり取りするための構成を備える。また、秘匿データを格納するために、通常の記録領域とは異なる機密データ記憶領域を設け、その機密データ記憶領域はストレージデバイス 2 0 0 内に設けられた暗号エンジンを介しないとアクセスできないように構成する。暗号エンジンは正当な権限を有すると認証されたホスト装置にのみ秘匿データを出力する。以下、このようなデータ保護機能を「セキュア機能」ともいう。上記の構成および機能により、ストレージデバイス 2 0 0 に記録された秘匿データを適切に保護することができる。

【 0 0 2 1 】

ストレージデバイス 2 0 0 のリムーバブルメディアとしての特徴を最大限に生かすため、通常データについては、セキュア機能に非対応のホスト装置でも入出力可能とするのが好ましい。そのため、本実施の形態のストレージデバイス 2 0 0 は、従来のハードディスクとの互換性を保つべく、ANSI (American National Standards Institute) の標準規格であるATA (AT Attachment) に対応しており、上述のセキュア機能は、ATAの拡張コマンドとして実現される。ATAはシングルタスクインタフェースを採用しており、一つの命令が発行されると、その命令が終了するまでバスが占有され、次の命令を発行できない。ところが、上述のように、ストレージデバイス 2 0 0 側にも暗号通信のための構成を設け、秘匿データを暗号化して入出力するようにすると、暗号化および復号などの処理には比較的長い時間を要するため、秘匿データの入出力命令に要する時間は、通常データの入出力命令に要する時間に比べて長くなる。たとえば、秘匿データをストレージデバイス 2 0 0 から読み出すとき、ストレージデバイス 2 0 0 に

対して読出命令を発行すると、ストレージデバイス 200 は、自身の暗号エンジンにより該当する秘匿データを機密データ記憶領域から読み出し、その秘匿データをホスト装置に送出するために用いる暗号鍵をホスト装置との間でやり取りした後、その秘匿データを暗号鍵で暗号化してからバスに出力する。このとき、暗号化および復号などの処理を実行している間は、バスは実際には使われていないにもかかわらず、この命令により占有された状態にある。

【0022】

本実施の形態では、このような無駄なバスの占有を極力省き、バスを効率良く利用して処理の高速化を図るために、秘匿データの入出力のための一連の暗号入出力処理を複数の手順に分割し、命令を細分化して発行する。そして、暗号化または復号など、バスを使わない処理が行われている間は、できる限りバスを開放して他の命令が発行できるようにする。

【0023】

ところが、秘匿データを入出力するための暗号入出力処理を複数の手順に分割したとき、それらの手順の実行順序が前後すると、セキュリティホールが発生する恐れがある。そのため、本実施の形態では、ストレージデバイス 200 の暗号エンジンは、秘匿データの入出力における命令の実行順序を管理し、不正な順序の命令を受信した場合、その命令の実行を拒否し、エラー応答を返す。また、本実施の形態では、記録装置 100、再生装置 300 が、複数の記録または再生処理を並行して実行することを想定し、ストレージデバイス 200 の処理能力に応じて複数の処理系を用意する。このとき、それぞれの処理系ごとに命令の実行順序を管理するために、それぞれの処理系の命令に処理系を識別するためのシーケンス ID を割り当て、シーケンス ID により、受信した命令がいずれの処理系に属する命令であるかを識別する。

【0024】

以下、秘匿データの入出力の例として、画像や音楽などのデジタルコンテンツを記録再生する場合について説明する。コンテンツ自身を秘匿データとして扱ってもよいが、本実施の形態では、コンテンツを暗号化し、暗号化されたコンテンツ自身は通常のデータとして入出力を行う。そして、暗号化されたコンテンツを

復号するための鍵（コンテンツ鍵と呼ぶ）を含む、コンテンツの復号および利用に必要なデータ（ライセンスデータと呼ぶ）を、秘匿データとして上述のセキュア機能を用いて入出力を行う。これにより、十分な耐タンパ性を維持しつつ、データの入出力を簡略化し、処理の高速化および消費電力の低減を図ることができる。以下、記録装置100、再生装置300などのホスト装置がストレージデバイス200に対して発行する命令のうち、セキュア機能のための命令を「セキュアコマンド」とも呼び、その他の命令を「通常コマンド」とも呼ぶ。

【0025】

図2は、実施の形態に係る記録装置100の内部構成を示す。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIなどで実現でき、ソフトウェア的にはメモリにロードされた記録制御機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。記録装置100は、主に、コントローラ101、ストレージインタフェース102、暗号エンジン103、暗号器104、コンテンツエンコーダ105、およびそれらを電氣的に接続するデータバス110を備える。

【0026】

コンテンツエンコーダ105は、オンラインまたはオフラインにより取得したコンテンツを所定の形式にエンコードする。たとえば、ネットワークを介して取得した画像データをJPEG形式にエンコードしてもよいし、放送波から取得した映像データをMPEG形式にエンコードしてもよい。暗号器104は、コンテンツを暗号化するための暗号鍵と、復号するためのコンテンツ鍵を発行し、エンコードしたコンテンツを暗号鍵で暗号化する。暗号化されたコンテンツは、データバス110およびストレージインタフェース102を介してストレージデバイス200に記録される。コンテンツ鍵は、暗号エンジン103に通知され、暗号エンジン103を介してストレージデバイス200に記録される。暗号エンジン103は、コンテンツ鍵を含むライセンスデータをストレージデバイス200に

入力するために、ストレージデバイス 200 との間で暗号通信の制御を行う。ストレージインタフェース 102 は、ストレージデバイス 200 とのデータの入出力を制御する。コントローラ 101 は、記録装置 100 の構成要素を統括的に制御する。

【0027】

図 3 は、実施の形態に係る再生装置 300 の内部構成を示す。これらの機能ブロックも、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。再生装置 300 は、主に、コントローラ 301、ストレージインタフェース 302、暗号エンジン 303、復号器 304、コンテンツデコーダ 305、およびそれらを電氣的に接続するデータバス 310 を備える。

【0028】

ストレージインタフェース 302 は、ストレージデバイス 200 とのデータの入出力を制御する。暗号エンジン 303 は、ライセンスキーを含むライセンスデータをストレージデバイス 200 から受信するために、ストレージデバイス 200 との間で暗号通信の制御を行う。復号器 304 は、ストレージデバイス 200 から読み出した暗号化されたコンテンツを、ストレージデバイス 200 から入手したライセンスデータに含まれるライセンスキーにより復号する。コンテンツデコーダ 305 は、復号器 304 により復号されたコンテンツをデコードして出力する。たとえば、画像データであれば、図示しない表示装置に出力し、音声データであれば、図示しないスピーカに出力する。コントローラ 301 は、再生装置 300 の構成要素を統括的に制御する。

【0029】

図 4 は、実施の形態に係るストレージデバイス 200 の内部構成を示す。ストレージデバイス 200 は、主に、コントローラ 201、ストレージインタフェース 202、暗号エンジン 203、通常データ記憶部 204、機密データ記憶部 205、およびそれらを電氣的に接続するデータバス 210 を備える。

【0030】

ストレージインタフェース 202 は、記録装置 100 および再生装置 300 と

のデータの入出力を制御する。暗号エンジン 2 0 3 は、コンテンツ鍵を含むライセンスデータなどの秘匿データを記録装置 1 0 0 および再生装置 3 0 0 との間で入出力するための制御を行う。通常データ記憶部 2 0 4 は、暗号化されたコンテンツや通常のデータなどを記録する。機密データ記憶部 2 0 5 は、コンテンツ鍵を含むライセンスデータなどの秘匿データを記録する。コントローラ 2 0 1 は、ストレージデバイス 2 0 0 の構成要素を統括的に制御する。通常データ記憶部 2 0 4 は、外部から直接アクセス（データの入出力）が行われるが、機密データ記憶部 2 0 5 は、暗号エンジン 2 0 3 により制御され、暗号エンジン 2 0 3 を介しないとアクセス（データの入出力）できないように構成される。

【0 0 3 1】

図 5 は、図 2 に示した記録装置 1 0 0 の暗号エンジン 1 0 3 の内部構成を示す。暗号エンジン 1 0 3 は、認証部 1 2 0、第 1 暗号部 1 2 1、乱数発生部 1 2 2、復号部 1 2 3、第 2 暗号部 1 2 4、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス 1 3 0 を備える。

【0 0 3 2】

認証部 1 2 0 は、ストレージデバイス 2 0 0 から取得した証明書を認証する。証明書は、公開鍵を含む平文の情報（証明書本体と呼ぶ）と、証明書本体に対して付される電子署名からなる。この電子署名は、証明書本体に対するハッシュ関数による演算結果を、第三者機関である認証局（図示せず）のルート鍵 K_{pa} によって暗号化したデータである。ルート鍵 K_{pa} は、認証局によって厳重に管理されている非公開な鍵であり、認証局の秘密鍵となる。認証部 1 2 0 は、このルート鍵 K_{pa} と対をなす認証鍵 K_Pa を保持している。この認証鍵 K_Pa は証明書の正当性を検証する公開鍵である。証明書の正当性の検証は、検証すべき証明書の証明書本体に対するハッシュ関数の演算結果と、認証鍵 K_Pa で電子署名を復号した結果を比較する処理であり、両者が一致したとき、正当であると判断する。この証明書の正当性を判断し、正当な証明書を承認する処理を認証と呼ぶ。認証部 1 2 0 は、認証に成功すると、ストレージデバイス 2 0 0 の公開鍵 K_Pc を取り出して第 1 暗号部 1 2 1 に伝達し、認証に失敗すると、エラー通知を出力する。

【0033】

乱数発生部122は、ストレージデバイス200との間で暗号通信を行うために一時的に使用されるチャレンジ鍵 K_s1 を発生する。暗号通信を行う度に、乱数によりチャレンジ鍵 K_s1 を生成することで、チャレンジ鍵 K_s1 を見破られる可能性を最小限に抑えることができる。生成されたチャレンジ鍵 K_s1 は、第1暗号部121および復号部123に伝達される。第1暗号部121は、ストレージデバイス200にチャレンジ鍵 K_s1 を通知するために、認証部120により取り出されたストレージデバイス200の公開鍵 K_Pc でチャレンジ鍵 K_s1 を暗号化して、暗号化共通鍵 $E(K_Pc, K_s1)$ を生成する。ここで、関数 E は暗号化を示し、 $E(K_Pc, K_s1)$ は、 K_Pc で K_s1 を暗号化したものであることを示す。

【0034】

復号部123は、チャレンジ鍵 K_s1 で暗号化されたデータを復号する。ストレージデバイス200で発行されたセッション鍵 K_s2 は、チャレンジ鍵 K_s1 により暗号化されてストレージデバイス200から供給されるため、復号部123は、乱数発生部122が発生したチャレンジ鍵 K_s1 を取得して、セッション鍵 K_s2 を復号する。復号したセッション鍵 K_s2 は第2暗号部124に伝達される。第2暗号部124は、暗号器104がコンテンツを暗号化する際に発行したコンテンツ鍵を含むライセンスデータを取得し、そのライセンスデータをストレージデバイス200で発行されたセッション鍵 K_s2 により暗号化する。

【0035】

図5では、暗号エンジン103の構成要素のうち、認証部120、第1暗号部121、復号部123、および第2暗号部124がローカルバス130により電氣的に接続されており、ローカルバス130を介して記録装置100のデータバス110に接続されている。各構成要素を接続する形態にはいろいろな変更例が考えられるが、本実施の形態では、チャレンジ鍵を発生する乱数発生部122が、直接データバス110に接続されないよう配慮している。これにより、暗号エンジン103内で使用される各鍵が、記録装置100の他の構成要素などを介して外部に漏洩することを防ぎ、セキュリティ性を向上させることができる。

【0036】

図6は、図3に示した再生装置300の暗号エンジン303の内部構成を示す。暗号エンジン303は、証明書出力部320、第1復号部321、暗号部322、乱数発生部323、第2復号部324、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス330を備える。

【0037】

証明書出力部320は、再生装置300の証明書を出力する。証明書は、証明書出力部320が保持してもよいし、図示しない証明書保持部に保持しておき、それを読み出してもよい。証明書は、再生装置300の公開鍵Kpbを含む証明書本体と、証明書本体に対して付される電子署名からなる。電子署名は、ストレージデバイス200の証明書と同様に、認証局のルート鍵Kpaにより暗号化されたデータである。第1復号部321は、公開鍵Kpbによって暗号化されたデータを秘密鍵Kpbで復号する。ストレージデバイス200で発行されたチャレンジ鍵Ks3は、再生装置300の公開鍵Kpbにより暗号化されてストレージデバイス200から供給されるため、第1復号部321は、自身の秘密鍵Kpbにより復号してチャレンジ鍵Ks3を取り出す。取り出されたチャレンジ鍵Ks3は、暗号部322に伝達される。乱数発生部323は、ストレージデバイス200との間で暗号通信を行うために一時的に使用されるセッション鍵Ks4を発生する。生成されたセッション鍵Ks4は、暗号部322および第2復号部324に伝達される。

【0038】

暗号部322は、ストレージデバイス200にセッション鍵Ks4を通知するために、復号部321により取り出されたチャレンジ鍵Ks3でセッション鍵Ks4を暗号化する。第2復号部324は、セッション鍵Ks4で暗号化されたデータを復号する。ライセンスデータは、セッション鍵Ks4により暗号化されてストレージデバイス200から供給されるため、第2復号部324は、乱数発生部323が発生したセッション鍵Ks4により復号して、ライセンスデータを取り出す。取り出されたライセンスデータは、復号器304に伝達され、復号器304はこのライセンスデータに含まれるコンテンツ鍵を用いて暗号化されたコン

テンツを復号する。

【 0 0 3 9 】

図 6 に示した暗号エンジン 3 0 3 においても、各構成要素を接続する形態にはいろいろな変更例が考えられるが、本実施の形態では、チャレンジ鍵を発生する乱数発生部 3 2 3 が直接データバス 3 1 0 に接続されないように構成することで、暗号エンジン 3 0 3 内で使用される暗号鍵が外部に漏洩することを防ぐ。

【 0 0 4 0 】

図 7 は、図 4 に示したストレージデバイス 2 0 0 の暗号エンジン 2 0 3 の内部構成を示す。これらの機能ブロックも、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。暗号エンジン 2 0 3 は、データレジスタ 2 2 0、状態レジスタ 2 2 1、制御部 2 2 2、内部レジスタ 2 2 3、乱数発生部 2 2 4、証明書出力部 2 2 5、認証部 2 2 6、第 1 復号部 2 2 7、第 1 暗号部 2 2 8、第 2 復号部 2 2 9、第 2 暗号部 2 3 0、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス 2 4 0 を備える。

【 0 0 4 1 】

データレジスタ 2 2 0 は、データ入出力用のレジスタであり、暗号エンジン 2 0 3 の外部の構成との間でデータの入出力を仲介する。状態レジスタ 2 2 1 は、コントローラ 2 0 1 が記録装置 1 0 0 または再生装置 3 0 0 から受信したセキュアコマンドの実行を暗号エンジン 2 0 3 に指示するための実行指示と、暗号エンジン 2 0 3 がセキュアコマンドの処理状態または処理結果などを示す状態情報や、実行中または実行済みの命令の種別を示す実行命令種別などを、コントローラ 2 0 1 に通知するための情報を保持する。

【 0 0 4 2 】

ストレージデバイス 2 0 0 のコントローラ 2 0 1 が、記録装置 1 0 0 または再生装置 3 0 0 のコントローラからセキュアコマンドを受信すると、状態レジスタ 2 2 1 にその命令の実行指示（開始指示）を格納する。たとえば、セキュアコマンドのそれぞれに実行順に番号を付しておき、コントローラ 2 0 1 が受信したセキュアコマンドの番号と、そのセキュアコマンドが属する処理系を示すシーケンス ID を状態レジスタ 2 2 1 に格納することで、暗号エンジン 2 0 3 に対して

そのコマンドの実行を指示する。制御部 2 2 2 は、状態レジスタ 2 2 1 に新しい実行指示が格納されると、その処理を開始する。

【 0 0 4 3 】

制御部 2 2 2 は、コントローラ 2 0 1 から通知された命令の処理状態および処理結果などを示すステータス情報を状態レジスタ 2 2 1 に格納する。処理状態は、たとえば、処理が実行されている状態を示す「B u s y」、処理が実行されていない状態を示す「R e a d y」の 2 つのステータスを示すフラグで表現することができ、処理結果は、たとえば、処理が正常に終了したことを示す「N o r m a l」、処理が異常終了したことを示す「E r r o r」の 2 つのステータスを示すフラグで表現することができる。状態レジスタ 2 2 1 に格納される実行命令種別は、実行指示と同様に、セキュアコマンドに付された番号とすることができる。

【 0 0 4 4 】

内部レジスタ 2 2 3 は、セキュアコマンドの実行に必要なテンポラルな秘密情報や命令に対する処理結果を処理系ごとに保持する。すなわち、内部レジスタ 2 2 3 は、処理系（シークエンス I D）ごとに秘密情報を保持する領域を備えている。テンポラルな秘密情報には、記録装置 1 0 0 または再生装置 3 0 0 との間の暗号通信に使用される鍵や、暗号化されない状態でのライセンスデータなどがある。

【 0 0 4 5 】

コントローラ 2 0 1 は、記録装置 1 0 0 または再生装置 3 0 0 のコントローラが発行したシークエンス I D が付されたセキュアコマンドを受信すると、状態レジスタ 2 2 1 を参照して、そのセキュアコマンドが属する処理系の処理状態をチェックし、セキュアコマンドの実行可否を判断する。その処理系の他の命令が実行中でなければ、暗号エンジン 2 0 3 に対して、その実行を指示するために、状態レジスタ 2 2 1 の実行指示に、受信したシークエンス I D と受信したセキュアコマンドの番号を格納する。

【 0 0 4 6 】

制御部 2 2 2 は、状態レジスタ 2 2 1 を参照し、状態レジスタ 2 2 1 に格納さ

れている実行指示に応じて暗号エンジン 2 0 3 内の他の構成要素に制御信号を伝達する。まず、制御部 2 2 2 は、状態レジスタ 2 2 1 から、実行指示として格納されたセキュアコマンドの番号とシーケンス ID を取得する。そして、再び、状態レジスタ 2 2 1 を参照して、そのセキュアコマンドが属する処理系の処理状態をチェックし、セキュアコマンドの実行可否を判断する。制御部 2 2 2 は、その処理系の直前の命令が正常に終了していて、かつ、受信した命令が正しい順序の命令であれば、その命令の実行を許可し、状態レジスタ 2 2 1 の実行命令種別をその命令の番号に変更し、状態情報を「B u s y」に変更する。制御部 2 2 2 は、その処理系の直前の命令が実行中か、異常終了か、または、受信した命令が不正な順序の命令であれば、その命令の実行を拒否し、状態レジスタ 2 2 1 の状態情報を「E r r o r」に変更する。このとき、不正な順序の命令が属する暗号入出力処理を中止してもよい。すなわち、状態レジスタ 2 2 1 の実行命令種別を初期化し、その暗号入出力処理は初めからやり直さない限り受け付けないようにしてもよい。これにより、不正なアクセスに対するセキュリティ性をより向上させることができる。なお、直前の命令における処理結果の影響を受けない命令もある。この場合には、その命令の実行は許可される命令もある。

【 0 0 4 7 】

乱数発生部 2 2 4 は、記録装置 1 0 0 または再生装置 3 0 0 との間の暗号通信に一時的に使用されるセッション鍵 K s 2 またはチャレンジ鍵 K s 3 を発生する。証明書出力部 2 2 5 は、ストレージデバイス 2 0 0 の証明書を出力する。証明書は、証明書出力部 2 2 5 が保持してもよいし、ストレージデバイス 2 0 0 の所定の記憶領域、たとえば機密データ記憶部 2 0 5 に保持しておき、それを読み出してもよい。証明書は、ストレージデバイス 2 0 0 の公開鍵 K P c を含む証明書本体と、証明書本体に付された電子署名とを含む。電子署名は、認証局のルート鍵 K p a により暗号化される。認証部 2 2 6 は、再生装置 3 0 0 から取得した証明書を認証する。認証部 2 2 6 は、証明書に含まれる電子署名を取り出して、認証鍵 K P a で、その正当性を認証する。認証部 2 2 6 は、認証に成功すると、証明書に含まれる再生装置 3 0 0 の公開鍵 K P b を取り出して内部レジスタ 2 2 3 に格納し、認証に失敗すると、制御部 2 2 2 へエラー通知を出力する。

【0048】

第1復号部227は、公開鍵暗号方式の公開鍵で暗号化されたデータを復号する。具体的には、自身の公開鍵K_{Pc}で暗号化されたデータを、自身の秘密鍵K_{pc}で復号する。第1暗号部228は、公開鍵暗号方式の公開鍵でデータを暗号化する。具体的には、再生装置300から受け取った再生装置300の公開鍵K_{Pb}で、乱数発生部224が発行したチャレンジ鍵K_{s3}を暗号化する。第2復号部229は、共通鍵暗号方式の鍵で暗号化されたデータを復号する。具体的には、乱数発生部224が発行したセッション鍵K_{s2}またはチャレンジ鍵K_{s3}で暗号化されたデータを、それぞれセッション鍵K_{s2}またはチャレンジ鍵K_{s3}で復号する。第2暗号部230は、共通鍵暗号方式の鍵でデータを暗号化する。具体的には、記録装置100が発行したチャレンジ鍵K_{s1}または再生装置300が発行したセッション鍵K_{s4}で、乱数発生部224が発行されたセッション鍵K_{s2}またはライセンスデータをそれぞれ暗号化する。

【0049】

つづいて、記録装置100がストレージデバイス200にライセンスデータを記録するまでの手順と、再生装置300がストレージデバイス200に記録されたライセンスデータを読み出すまでの手順を概説し、その後、本実施の形態に係る複数のシーケンスの並列処理について詳述することにする。

【0050】

図8および図9は、記録装置100がストレージデバイス200にライセンスデータを記録するまでの一連の暗号入出力処理の手順を示す。記録装置100のコントローラ101は、ストレージデバイス200に暗号入出力処理を実行させるために、ストレージデバイス200に対してセキュアコマンドを発行する。ストレージデバイス200のコントローラ101は、記録装置100からセキュアコマンドを受信すると、状態レジスタ221を介して、暗号エンジン203の制御部222にセキュアコマンドの実行を指示する。記録装置100と暗号エンジン203の間でデータを交換する場合も、同様にコントローラ201とデータレジスタ220を介してデータが交換される。ここでは、説明を簡単にするため、記録装置100とストレージデバイス200の暗号エンジン203の間で一連の

暗号入出力処理が実行されるものとして説明を行う。

【0051】

まず、記録装置100のコントローラ101と、ストレージデバイス200の暗号エンジン203との間で、シークエンスIDを確保する処理が行われる（S100）。この処理の詳細については、図13および図14において詳述する。ここでは、シークエンスID「1」が確保されたことにして説明を進める。シークエンスIDが確保されると、コントローラ101は、暗号エンジン203に対して証明書出力命令（シークエンスID=1）を発行する（S102）。暗号エンジン203が証明書出力命令を正常に受理すると（S104）、制御部222は、証明書出力部225により証明書を読み出してコントローラ101へ送る（S106）。ここで、暗号エンジン203が証明書出力命令を正常に受理できなかったときは、暗号エンジン203はコントローラ101にエラー通知を返すが、この処理の詳細については後述する。

【0052】

コントローラ101は、ストレージデバイス200から証明書を取得すると、それを記録装置100の暗号エンジン103に送る（S108）。暗号エンジン103がストレージデバイス200の証明書を受信すると（S110）、認証部120は、認証鍵K_{P a}で、取得した証明書の正当性を認証する（S112）。証明書が承認されなかった場合は（S112のN）、認証部120はエラー通知をコントローラ101に送信する（S190）。コントローラ101は、エラー通知を受信すると（S192）、処理を異常終了する。

【0053】

証明書が承認された場合は（S112のY）、暗号エンジン103は、乱数発生部122により、チャレンジ鍵K_{s 1}を発生し（S114）、第1暗号部121により、証明書から取り出されたストレージデバイス200の公開鍵K_{P c}でチャレンジ鍵K_{s 1}を暗号化して暗号化共通鍵E（K_{P c}、K_{s 1}）を生成し、コントローラ101へ送る（S116）。コントローラ101は、暗号化共通鍵E（K_{P c}、K_{s 1}）を受信すると（S118）、暗号エンジン203に対してチャレンジ鍵入力命令（シークエンスID=1）を発行する（S120）。暗号

エンジン 203 がチャレンジ鍵入力命令を正常に受理すると (S122)、コントローラ 101 は、暗号化共通鍵 E (K_{Pc}、K_{s1}) を暗号エンジン 203 へ出力する (S124)。暗号エンジン 203 が暗号化共通鍵 E (K_{Pc}、K_{s1}) を受信すると (S126)、制御部 222 により、受信した暗号化共通鍵 E (K_{Pc}、K_{s1}) を第 1 復号部 227 に与える。第 1 復号部 227 は、自身の秘密鍵 K_{pc} で暗号化共通鍵 E (K_{Pc}、K_{s1}) を復号してチャレンジ鍵 K_{s1} を取り出し (S128)、制御部 222 へ与える。制御部 222 は、内部レジスタ 223 のシークエンス ID=1 の領域にチャレンジ鍵 K_{s1} (シークエンス ID=1) を格納する (S130)。

【0054】

つづいて、コントローラ 101 は、暗号エンジン 203 に対してセッション鍵準備命令 (シークエンス ID=1) を発行する (S132)。暗号エンジン 203 がセッション鍵準備命令を正常に受理すると (S134)、乱数発生部 224 は、セッション鍵 K_{s2} を発生し、制御部 222 へ与える。制御部 222 は、内部レジスタ 223 のシークエンス ID=1 の領域にセッション鍵 K_{s2} (シークエンス ID=1) を格納する (S138)。つづいて、制御部 222 は、内部レジスタ 223 のシークエンス ID=1 の領域からチャレンジ鍵 K_{s1} (シークエンス ID=1) を読み出し、乱数発生部 224 が生成したセッション鍵 K_{s2} (シークエンス ID=1) と内部レジスタ 223 から読み出したチャレンジ鍵 K_{s1} (シークエンス ID=1) とを第 2 暗号部 230 に与える。第 2 暗号部 230 は、セッション鍵 K_{s2} (シークエンス ID=1) をチャレンジ鍵 K_{s1} (シークエンス ID=1) で暗号化して暗号化共通鍵 E (K_{s1}、K_{s2}) を生成し、内部レジスタ 223 のシークエンス ID=1 の領域に格納する (S140)。

【0055】

つづいて、コントローラ 101 は、暗号エンジン 203 に対してセッション鍵出力命令 (シークエンス ID=1) を発行する (S142)。暗号エンジン 203 は、セッション鍵出力命令を正常に受理すると (S144)、内部レジスタ 223 のシークエンス ID=1 の領域から暗号化共通鍵 E (K_{s1}、K_{s2}) を読み出して、コントローラ 101 に出力する (S146)。コントローラ 101 は

、ストレージデバイス 200 から暗号化共通鍵 E (Ks1、Ks2) を受信すると、それを暗号エンジン 103 に送る (S148)。暗号エンジン 103 がコントローラ 101 から暗号化共通鍵 E (Ks1、Ks2) を受信すると (S150)、復号部 123 は、乱数発生部 122 が発生したチャレンジ鍵 Ks1 で暗号化共通鍵 E (Ks1、Ks2) を復号してセッション鍵 Ks2 を取り出す (S152)。

【0056】

つづいて、暗号エンジン 103 は、第 2 暗号部 124 により、暗号器 104 が発行したコンテンツのコンテンツ鍵を含むライセンスデータを、復号部 123 が取り出したセッション鍵 Ks2 で暗号化して暗号化ライセンスデータを生成し、コントローラ 101 に送る (S154)。コントローラ 101 は、暗号化ライセンスデータを受信すると (S156)、暗号エンジン 203 に対してライセンスデータ入力命令 (シーケンス ID=1) を発行する (S158)。暗号エンジン 203 がライセンスデータ入力命令を正常に受理すると (S160)、コントローラ 101 は、暗号化ライセンスデータを暗号エンジン 203 へ出力する (S162)。暗号エンジン 203 が暗号化ライセンスデータを受信すると (S164)、制御部 222 は、受信した暗号化ライセンスデータを第 2 復号部 229 へ与えるとともに、内部レジスタ 223 のシーケンス ID=1 の領域からセッション鍵 Ks2 (シーケンス ID=1) を読み出して第 2 復号部 229 へ与える。第 2 復号部 229 は、セッション鍵 Ks2 (シーケンス ID=1) で暗号化ライセンスデータを復号して、ライセンスデータを取り出す。制御部 222 は、ライセンスデータを内部レジスタ 223 のシーケンス ID=1 の領域へ格納する (S166)。

【0057】

つづいて、コントローラ 101 は、暗号エンジン 203 に対してライセンスデータ書込命令 (シーケンス ID=1) を発行し、ライセンスデータの書込アドレスを指定する (S168)。暗号エンジン 203 がライセンスデータ書込命令を正常に受理すると (S170)、制御部 222 は、内部レジスタ 223 のシーケンス ID=1 の領域に格納されたライセンスデータを読み出し、機密データ

記憶部 205 の指定されたアドレスに格納する (S172)。最後に、コントローラ 101 と暗号エンジン 203 との間で、シーケンス ID を開放する処理が行われる (S174)。この処理の詳細については、図 15 において詳述する。以上の手順により、コンテンツを復号するためのライセンスデータがストレージデバイス 200 に記録される。

【0058】

本実施の形態では、前述したように、ライセンスデータを記録するための暗号入出力処理を、証明書出力命令 (S102)、チャレンジ鍵入力命令 (S120)、セッション鍵準備命令 (S132)、セッション鍵出力命令 (S142)、ライセンスデータ入力命令 (S158)、ライセンス書込命令 (S168) のセキュアコマンドに分割し、一連の暗号入出力処理にシーケンス ID を割り当てる。これにより、複数の暗号入出力処理を並列して実行しても、どの処理系に属するセキュアコマンドなのかを識別可能としているので、セキュアコマンドの実行順序を適切に管理し、かつ、セキュアコマンドによってやり取りされた鍵やデータを処理系ごとに安全に管理することができる。

【0059】

図 10 および図 11 は、再生装置 300 がストレージデバイス 200 からライセンスデータを読み出すまでの手順を示す。図 8 および図 9 に示した記録装置 100 がストレージデバイス 200 にライセンスデータを記録するまでの手順と同様に、再生装置 300 のコントローラ 301 が、ストレージデバイス 200 に暗号入出力処理を実行させるためにセキュアコマンドを発行したとき、ストレージデバイス 200 のコントローラ 201 および状態レジスタ 221 を介して暗号エンジン 203 にコマンドが伝達されるが、ここでは、説明を簡単にするため、再生装置 300 と暗号エンジン 203 の間で一連の暗号入出力処理が実行されるものとして説明を行う。

【0060】

まず、再生装置 300 のコントローラ 301 と、ストレージデバイス 200 の暗号エンジン 203 との間で、シーケンス ID を確保する処理が行われる (S200)。この処理の詳細については、図 13 および図 14 において詳述する。

ここでは、シーケンス ID「2」が確保されたことにして説明を進める。シーケンス ID が確保されると、再生装置 300 の暗号エンジン 303 は、証明書出力部 320 により、証明書をコントローラ 301 へ送る (S202)。コントローラ 301 は、暗号エンジン 303 から証明書を受信すると (S204)、暗号エンジン 203 に対して証明書入力命令 (シーケンス ID=2) を発行する (S206)。暗号エンジン 203 が証明書入力命令を正常に受理すると (S208)、コントローラ 301 は暗号エンジン 203 に証明書を出力する (S210)。ここで、暗号エンジン 203 が証明書入力命令を正常に受理できなかったときは、暗号エンジン 203 はコントローラ 301 にエラー通知を返すが、この処理の詳細については後述する。

【0061】

暗号エンジン 203 が再生装置 300 の証明書を受信すると (S212)、認証部 226 は、認証鍵 KPa で取得した証明書の正当性を認証する。 (S214)。証明書が承認されなかった場合は (S214 の N)、認証部 226 はエラー通知をコントローラ 301 に送信する (S290)。コントローラ 301 は、エラー通知を受信すると (S292)、処理を異常終了する。

【0062】

証明書が承認された場合は (S214 の Y)、制御部 222 は、証明書から再生装置 300 の公開鍵 K Pb を取り出して、内部レジスタ 223 のシーケンス ID=2 の領域に格納する (S216)。つづいて、コントローラ 301 は、暗号エンジン 203 に対してチャレンジ鍵準備命令 (シーケンス ID=2) を発行する (S218)。暗号エンジン 203 が、チャレンジ鍵準備命令を正常に受理すると (S220)、乱数発生部 224 はチャレンジ鍵 K s 3 を発生し、制御部 222 に与える。制御部 222 は、それを内部レジスタ 223 のシーケンス ID=2 の領域に格納する (S222)。そして、制御部 222 は、生成したチャレンジ鍵 K s 3 と、内部レジスタ 223 のシーケンス ID=1 の領域から読み出した再生装置 300 の公開鍵 K Pb (シーケンス ID=1) を第 1 暗号部 228 に与える。そして、第 1 暗号部 228 は、与えられたチャレンジ鍵 K s 3 を再生装置 300 の公開鍵 K Pb で暗号化して暗号化鍵 E (K Pb、K s 3) を

生成し、内部レジスタ 223 のシークエンス ID=2 領域に一時格納する (S244)。つづいて、コントローラ 301 は、暗号エンジン 203 に対してチャレンジ鍵出力命令 (シークエンス ID=2) を発行する (S226)。暗号エンジン 203 がチャレンジ鍵出力命令を正常に受理すると (S228)、制御部 222 は、暗号化鍵 E (Kpb、Ks3) を内部レジスタ 223 のシークエンス ID=1 の領域から読み出し、コントローラ 301 へ出力する (S230)。

【0063】

コントローラ 301 は、暗号化共通鍵 E (Kpb、Ks3) を受信すると、それを暗号エンジン 303 に送る (S232)。暗号エンジン 303 が暗号化共通鍵 E (Kpb、Ks3) を受信すると、第 1 復号部 321 は、暗号化共通鍵 E (Kpb、Ks3) を自身の秘密鍵 Kpb で復号してチャレンジ鍵 Ks3 を取り出す (S236)。つづいて、暗号エンジン 303 は、乱数発生部 323 によりセッション鍵 Ks4 を発生し (S238)、暗号部 322 によりチャレンジ鍵 Ks3 でセッション鍵 Ks4 を暗号化して暗号化共通鍵 E (Ks3、Ks4) を生成し、コントローラ 301 へ送る (S240)。コントローラ 301 は、暗号化共通鍵 E (Ks3、Ks4) を受信すると (S242)、暗号エンジン 203 に対してセッション鍵入力命令 (シークエンス ID=2) を発行する (S244)。暗号エンジン 203 がセッション鍵入力命令を正常に受理すると (S246)、コントローラ 301 は、暗号化共通鍵 E (Ks3、Ks4) を暗号エンジン 203 へ出力する (S248)。暗号エンジン 203 が暗号化共通鍵 E (Ks3、Ks4) を受信すると (S250)、制御部 222 は、内部レジスタ 223 のシークエンス ID=2 の領域からチャレンジ鍵 Ks3 (シークエンス ID=2) を読み出し、第 2 復号部 229 に、受信した暗号化共通鍵 E (Ks3、Ks4) とチャレンジ鍵 Ks3 (シークエンス ID=2) を与える。第 2 復号部 229 は、チャレンジ鍵 Ks3 (シークエンス ID=2) で暗号化共通鍵 E (Ks3、Ks4) を復号してセッション鍵 Ks4 を取り出し (S252)、内部レジスタ 223 のシークエンス ID=2 の領域にセッション鍵 Ks4 (シークエンス ID=2) を格納する (S254)。

【0064】

つづいて、コントローラ 301 は、暗号エンジン 203 に対してライセンス読出命令（シーケンス ID=2）を発行し、ライセンスデータの読出アドレスを指定する（S256）。暗号エンジン 203 は、ライセンスデータ読出命令を正常に受理すると（S258）、制御部 222 により、ライセンスデータを機密データ記憶部 205 の指定されたアドレスから読み出して、内部レジスタ 223 のシーケンス ID=2 の領域に一時格納する（S260）。つづいて、コントローラ 301 は、暗号エンジン 203 に対してライセンス準備命令（シーケンス ID=2）を発行する（S262）。暗号エンジン 203 がライセンスデータ準備命令を正常に受理すると（S264）、制御部 222 は、内部レジスタ 223 のシーケンス ID=2 の領域から、ライセンスデータとセッション鍵 Ks4（シーケンス ID=2）を読み出し、第 2 暗号部 230 へ与える。第 2 暗号部 230 は、セッション鍵 Ks4 でライセンスデータを暗号化し、暗号化ライセンスデータを生成して（S266）、内部レジスタ 223 のシーケンス ID=2 の領域に一時格納する。

【0065】

つづいて、コントローラ 301 は、暗号エンジン 203 に対してライセンス出力命令（シーケンス ID=2）を発行する（S268）。暗号エンジン 203 は、ライセンスデータ出力命令を正常に受理すると（S270）、暗号化ライセンスデータをコントローラ 301 に出力する（S272）。コントローラ 301 が暗号化ライセンスデータを取得すると（S274）、コントローラ 301 と暗号エンジン 203 との間で、シーケンス ID を開放する処理が行われる（S276）。この処理の詳細については、図 15 において詳述する。つづいて、コントローラ 301 は、暗号化ライセンスデータを暗号エンジン 303 に送る（S278）。暗号エンジン 303 が暗号化ライセンスデータを受信すると（S280）、第 2 復号部 324 は、セッション鍵 Ks4 で暗号化ライセンスデータを復号する（S282）。得られたライセンスデータは、復号器 304 に送られ、復号器 304 がコンテンツを復号するのに用いられる。以上の手順により、コンテンツを復号するためのライセンスデータが再生装置 300 により読み出される。

【0066】

本実施の形態では、前述したように、ライセンスデータを読み出すための暗号入出力処理を、証明書入力命令（S204）、チャレンジ鍵準備命令（S218）、チャレンジ鍵出力命令（S226）、セッション鍵入力命令（S244）、ライセンス読出命令（S256）、ライセンス準備命令（S262）、ライセンス出力命令（S268）のセキュアコマンドに分割し、一連の暗号入出力処理にシーケンスIDを割り当てる。これにより、複数の暗号入出力処理を並列して実行しても、どの処理系に属するセキュアコマンドなのかを識別可能としているので、セキュアコマンドの実行順序を適切に管理し、かつ、セキュアコマンドによってやり取りされた鍵やデータを処理系ごとに安全に管理することができる。

【0067】

図12は、ホスト装置とストレージデバイスとの間で並列して処理可能な処理系の数を決定する手順を示す。ストレージデバイス200が記録装置100に接続されると、記録装置100のコントローラ101は、ストレージデバイスにデバイス情報出力命令を発行する（S300）。ストレージデバイス200のコントローラ201は、記録装置100のコントローラ101からデバイス情報出力命令を受信すると（S302）、デバイス情報を出力する（S304）。デバイス情報として、たとえば、ハードディスクの種類、通常データの記録容量、インタフェースの条件、サポートするコマンドセットなどの情報が通知される。コントローラ101は、ストレージデバイス200のデバイス情報を受信すると（S306）、ストレージデバイス200がセキュアコマンドセットをサポートしているか否かを判断し（S308）、サポートしていなければ（S308のN）、従来のハードディスクと同様に取り扱う。

【0068】

ストレージデバイス200がセキュアコマンドセットをサポートしていれば（S308のY）、つづいて、コントローラ101は、セキュア情報出力命令を発行する（S310）。コントローラ201は、セキュア情報出力命令を受信すると（S312）、セキュア情報を出力する（S314）。セキュア情報として、たとえば、セキュアコマンドに用いられる暗号アルゴリズムや証明書に関する情報、セキュアコマンドの実行に要する時間などが通知される。さらに、セキュア

情報には、並行して処理可能な処理系の上限、すなわち、利用可能なシークエンス ID に関する情報が含まれている。コントローラ 1 0 1 は、ストレージデバイス 2 0 0 のセキュア情報を受信すると (S 3 1 6)、ストレージデバイス 2 0 0 において並行して処理可能な処理系の上限や、ストレージデバイスにおける暗号処理時間などのライセンスデータの入出力に関する性能情報をセキュア情報から取り出して、取り出した性能情報と自身の性能に基づき記録装置 1 0 0 において利用する処理系の数を決定する (S 3 1 8)。そして、決定した範囲内でライセンスデータの記録を行う。決定された処理系の数は、ストレージデバイス 2 0 0 に通知されてもよい。

【0 0 6 9】

図 1 3 は、暗号入出力処理の実行に先立って、その暗号入出力処理を識別するためのシークエンス ID を確保する手順、すなわち、図 8 の S 1 0 0、および、図 1 0 の S 2 0 0 における処理の手順を示す。図 1 3 は、記録装置 1 0 0 のコントローラ 1 0 1 または再生装置 3 0 0 のコントローラ 3 0 1 側で、シークエンス ID を管理するために必要な情報を得るための処理例を示す。図 1 3 では、記録装置 1 0 0 とストレージデバイス 2 0 0 との間でシークエンス ID を確保する手順について説明するが、再生装置 3 0 0 とストレージデバイス 2 0 0 との間でシークエンス ID を確保する場合も同様である。

【0 0 7 0】

まず、コントローラ 1 0 1 は、図 1 2 の手順で取得した使用可能なシークエンス ID の候補の中から、未使用のシークエンス ID を選出し (S 4 0 0)、そのシークエンス ID を用いて、ストレージデバイス 2 0 0 に対してシークエンス確保命令を発行する (S 4 0 2)。ストレージデバイス 2 0 0 の暗号エンジン 2 0 3 は、記録装置 1 0 0 からシークエンス確保命令 (ID = x) を受信すると (S 4 0 6)、状態レジスタ 2 2 1 を参照して、そのシークエンス ID の処理系の処理状態を確認し、そのシークエンス ID が確保可能か否かを判断する (S 4 0 8)。シークエンス ID = x が既に確保中 (状態情報が「B u s y」、「N o r m a l」、「E r r o r」の場合) であるか、または、使用可能なシークエンス ID の範囲外であったときは (S 4 0 8 の N)、コントローラ 1 0 1 にエラーを通

知する (S412)。シークエンス ID「x」が開放中 (状態情報が「Ready」の場合) であれば (S408のY)、そのシークエンス IDに対応する処理系を確保するために、暗号エンジン 203 にその旨を通知する。制御部 222 は、状態レジスタ 221 の当該シークエンス IDに対応する領域を初期化し、状態情報を「Normal」に変更する (S408)。そして、シークエンス IDを確保した旨をコントローラ 101 に通知する (S410)。コントローラ 101 は、暗号エンジン 203 からの通知を受信すると (S414)、通知の内容を確認する (S416)。シークエンス IDを確保した旨の通知であれば (S416のY)、処理を終了する。エラー通知であれば (S416のN)、使用可能な全てのシークエンス IDについて処理が終了しているか否かを判断し (S418)、処理が終了していれば (S418のY)、いったん処理を終了し、シークエンス IDが開放されるまで待機する。そうでなければ (S418のN)、S400に戻り、別のシークエンス IDを用いてシークエンス確保命令を発行する。

【0071】

図 14 は、暗号入出力処理の実行に先立って、その暗号入出力処理を識別するためのシークエンス IDを確保する別の手順を示す。図 14 は、ストレージデバイス 200 の暗号エンジン 203 側で、使用するシークエンス IDを決定する例を示す。図 14 でも、記録装置 100 とストレージデバイス 200 との間でシークエンス IDを確保する手順について説明するが、再生装置 300 とストレージデバイス 200 との間でシークエンス IDを確保する場合も同様である。

【0072】

まず、コントローラ 101 は、ストレージデバイス 200 に対してシークエンス確保命令を発行する (S500)。ストレージデバイス 200 の暗号エンジン 203 は、記録装置 100 からシークエンス確保命令を受信すると (S502)、状態レジスタ 221 を参照して、開放中のシークエンス IDの有無を確認する (S504)。使用可能な全てのシークエンス IDが確保中 (状態情報が「Busy」、「Normal」、「Error」) であれば (S504のN)、コントローラ 101 にエラーを通知する (S512)。開放中 (状態情報が「Ready」) で確保可能なシークエンス IDがあれば (S504のY)、その中から

シーケンス ID を選択し (S506)、そのシーケンス ID に対応する処理系を確保するために、制御部 222 は状態レジスタ 221 の当該シーケンス ID に対応する領域を初期化し、状態情報を「Normal」に変更する (S508)。そして、確保したシーケンス ID をコントローラ 101 に通知する (S510)。コントローラ 101 は、暗号エンジン 203 からの通知を受信すると (S514)、通知の内容を確認する (S516)。シーケンス ID を確保した旨の通知であれば (S516 の Y)、処理を終了する。エラー通知であれば (S516 の N)、いったん処理を終了し、シーケンス ID が開放されるまで待機する。

【0073】

なお、シーケンス ID の確保の手順として、図 13、図 14 の 2 つの手順を示したが、ストレージデバイス 200 は、必ずしも両手順に対応している必要はない。いずれか 1 つに対応していても、両手順に対応していてもよい。

【0074】

図 15 は、シーケンス ID を開放する手順を示す。図 15 では、記録装置 100 がストレージデバイス 200 にシーケンス ID の開放を要求する手順について説明するが、再生装置 300 がストレージデバイス 200 シーケンス ID の開放を要求する場合も同様である。記録装置 100 のコントローラ 101 は、一連の暗号入出力処理の実行が終了すると、そのシーケンス ID のシーケンス開放命令を発行する (S600)。ストレージデバイス 200 の暗号エンジン 203 は、記録装置 100 からシーケンス開放命令 (ID=x) を受信すると (S602)、そのシーケンス ID に対応する処理系を開放し (S604)、状態レジスタ 221 の該当するシーケンス ID に対する状態情報を「Ready」に変更する。そして、開放した旨を記録装置 100 に通知する (S606)。コントローラ 101 は、ストレージデバイス 200 から通知を受信すると (S608)、処理を終了する。

【0075】

図 16 は、暗号エンジン 203 が、ホスト装置が発行したセキュアコマンド (以下「シーケンス命令」ともいう) を受理する手順を示す。図 16 では、記録

装置 100 が発行したセキュアコマンドをストレージデバイス 200 が受理する手順について説明するが、再生装置 300 が発行したセキュアコマンドをストレージデバイス 200 が受理する場合も同様である。まず、記録装置 100 のコントローラ 101 がシークエンス命令 (ID=x) を発行する (S700)。ストレージデバイス 200 の暗号エンジン 203 が記録装置 100 からシークエンス命令 (ID=x) を受信すると (S702)、制御部 222 が状態レジスタ 221 の当該シークエンス ID に対する状態情報を参照して、そのシークエンス ID に対応する処理系の状態を確認し、命令の実行が可能か否かを判断する (S704)。状態情報によって、そのシークエンス ID が開放中であるか、先の命令が異常終了していると確認されたとき、または、使用可能なシークエンス ID の範囲外であったときは、命令の実行は不可であると判断され (S704 の N)、コントローラ 101 にエラーを通知する (S710)。ただし、命令によっては先の命令が異常終了していても命令の実行が可能であると判断されるものもある。たとえば、シークエンス開放命令 (図 12 の S300、図 13 の S402)、証明書出力命令 (図 8 の S102)、証明書入力命令 (図 10 の S208) などがそれにあたる。

【0076】

そのシークエンス ID の状態情報によって命令の実行が可能であると判断される場合は (S704 の Y)、さらに、制御部 222 は状態レジスタ 221 の当該シークエンス ID に対する実行命令種別を参照して、受信したシークエンス命令の発行順が正しいか否かを確認する (S706)。シークエンス命令の順序が不正であれば (S706 の N)、コントローラ 101 にエラーを通知する (S710)。シークエンス命令の順序が正しければ (S708 の Y)、コントローラ 101 に命令を受理する旨を通知する (S708)。コントローラ 101 は、ストレージデバイス 200 からの通知を受信すると (S712)、通知の種類を確認し (S714)、受理通知であれば (S712 の Y)、続けて次の処理に移り、エラー通知であれば (S712 の N)、異常終了する。

【0077】

一方、命令を受理したストレージデバイス 200 では、当該シークエンス ID

に対応する処理系の状態情報が「N o r m a l」の場合、および、「B u s y」から「N o r m a l」に移行した場合、制御部 2 2 2 は、当該シーケンス I D に対応する処理系の状態情報を「B u s y」に、実行命令種別を当該命令の番号に変更し、処理を開始する。状態情報が「B u s y」から「E r r o r」に移行した場合には、受理した命令は実行されない。そして、当該シーケンス I D に対応する処理系の次のシーケンス命令を受信した時に、再び図 1 6 の手順によって、当該シーケンス I D に対する命令の異常終了が確認され、S 7 1 0 によってエラーが通知される。

【 0 0 7 8 】

暗号エンジン 2 0 3 は、不正なシーケンス命令を受信したときに、その処理系の処理を強制終了してもよい。すなわち、状態レジスタ 2 2 1 の該当シーケンス I D に対応する領域を初期化してもよい。これにより、不正な命令に対して処理を続行する恐れを抑え、耐タンパ性を向上させることができる。この場合、シーケンス命令で何らかのエラーが発生したとき、再度その暗号入出力処理を実行するには、記録装置 1 0 0 は、最初のシーケンス命令からやり直す必要がある。別の例では、通信ログを記録し、記録された通信ログを参照して正当なシーケンス命令が実行されていたことを認証できた場合は、その次のシーケンス命令から続行できるようにしてもよい。

【 0 0 7 9 】

図 1 7 は、ホスト装置からストレージデバイス 2 0 0 へ命令が発行される様子を示す。図 1 7 の例では、ホスト装置とストレージデバイス 2 0 0 との間の暗号入出力処理について 3 つの処理系が用意されており、ホスト装置は、シーケンス I D = 1、2、および 3 で識別されるシーケンス命令と、通常命令とを、並行してストレージデバイス 2 0 0 に対して発行する。ストレージデバイス 2 0 0 は、受信した命令を次々に処理していくが、図示したように、それぞれの処理系の中では、シーケンス命令をシーケンス I D により識別しつつ、適切に実行順序をチェックして処理を進める。

【 0 0 8 0 】

以上の説明は、シーケンス I D で管理される全ての処理系列が、ここまでに

記してきた方法に従ってライセンス入出力を行うことを想定したものである。しかし、シークエンスIDが割り当てられた個々の処理系列が、各々別個の処理体系に基づいてライセンスの入出力を行えるようにしても良い。これを実現するために、シークエンスIDを確保する際、ライセンス入出力を行うための処理体系をホストが指定できるようにする。以下では、ここで指定される処理体系のことを、処理モードと呼ぶ。シークエンスIDに処理体系が割り当てられた後では、受信した命令が指定された処理系のものであるか、そしてそれが正しい順序で発行されたものであるかどうかを、ストレージデバイス200が判断する。これらのどちらか一方の条件でも満たされなかった場合は、ストレージデバイス200は、受信した命令に対する応答としてエラーを返すか、処理系列を中断する。

【0081】

(第2の実施の形態)

図18は、第2の実施の形態に係るデータ管理システム10の全体構成を示す。本実施の形態では、第1の実施の形態における記録装置100および再生装置300が一つの記録再生装置400として実現されている。

【0082】

図19は、本実施の形態に係る記録再生装置400の内部構成を示す。本実施の形態の記録再生装置400は、図2に示した第1の実施の形態の記録装置100の構成と、図3に示した第1の実施の形態の再生装置300の構成の双方を備えており、同様の構成には同じ符号を付している。第1暗号エンジン103は、第1の実施の形態における記録装置100の暗号エンジン103に対応し、第2暗号エンジン303は、第1の実施の形態における再生装置300の暗号エンジン303に対応する。第1暗号エンジン103の内部構成は、図5に示した第1の実施の形態の暗号エンジン103と同様であり、第2暗号エンジン303の内部構成は、図6に示した第1の実施の形態の暗号エンジン303の内部構成と同様である。コントローラ401は、第1の実施の形態における記録装置100のコントローラ101と再生装置300のコントローラ301の双方の機能を有する。ストレージインタフェース402は、ストレージデバイス200とのデータの入出力を制御し、データバス410は、記録再生装置400の構成を電氣的に

接続する。

【0083】

本実施の形態の記録再生装置 400 の動作も、第 1 の実施の形態と同様であり、第 1 の実施の形態で説明した動作において、記録装置 100 を記録再生装置 400 に、暗号エンジン 103 を第 1 暗号エンジン 103 に、コントローラ 101 をコントローラ 401 に、再生装置 300 を記録再生装置 400 に、暗号エンジン 303 を第 2 暗号エンジン 303 に、コントローラ 301 をコントローラ 401 にそれぞれ置き換えたものと同様である。

【0084】

図 20 は、記録再生装置 400 からストレージデバイス 200 へ命令が発行される様子を示す。図 20 では、図 8 から図 11 に示したライセンスデータの記録および読み出しが並行して実行されている。ストレージデバイス 200 は、並行して発行される各種の命令をシークエンス ID により識別しつつ、適切に実行順序をチェックして処理を進める。

【0085】

(第 3 の実施の形態)

図 21 は、第 3 の実施の形態に係る記録装置 100 の内部構成を示す。本実施の形態では、第 1 の実施の形態における記録装置 100 が、コンテンツを配信する配信サーバ 150 とコンテンツの提供を受ける端末装置 160 として実現されている。配信サーバ 150 は、暗号エンジン 103、通信装置 152、コンテンツデータベース 153、ライセンスデータベース 154、ユーザデータベース 155、それらを制御するコントローラ 151、およびそれらを電氣的に接続するデータバス 156 を備える。端末装置 160 は、コントローラ 101、ストレージインタフェース 102、通信装置 162、およびそれらを電氣的に接続するデータバス 166 を備える。配信サーバ 150 と端末装置 160 は、それぞれ通信装置 152 および 162 を介して、ネットワークの一例としてのインターネット 20 により接続される。配信サーバ 150 の暗号エンジン 103 は、第 1 の実施の形態の暗号エンジン 103 と同様の機能を有し、端末装置 160 のコントローラ 101 およびストレージインタフェース 102 は、それぞれ第 1 の実施の形態

のコントローラ 1 0 1 およびストレージインタフェース 1 0 2 と同様の機能を有する。

【 0 0 8 6 】

コンテンツデータベース 1 5 3 は、ユーザに提供するコンテンツを保持する。ライセンスデータベース 1 5 4 は、コンテンツを暗号化するのに用いられるコンテンツ鍵を含むライセンスデータを保持する。本実施の形態では、コンテンツは既にコンテンツ鍵により暗号化されてコンテンツデータベース 1 5 3 に格納されているが、コンテンツデータベース 1 5 3 に暗号化される前のコンテンツデータを格納しておき、配信サーバ 1 5 0 に第 1 の実施の形態におけるコンテンツエンコード 1 0 5 および暗号器 1 0 4 をさらに設け、コンテンツデータベース 1 5 3 からコンテンツを読み出してエンコードし、暗号化してもよい。ユーザデータベース 1 5 5 は、コンテンツを提供するユーザの情報を保持する。たとえば、ユーザの個人情報、端末装置 1 6 0 のアドレス、コンテンツの購入履歴、課金情報などを保持してもよい。コントローラ 1 5 1 は、ユーザからの要求に応じて暗号化されたコンテンツをコンテンツデータベース 1 5 3 から読み出してユーザに提供する。そして、暗号エンジン 1 0 3 によりそのコンテンツを復号するためのライセンスデータがユーザに提供されると、そのコンテンツの対価を課金すべくユーザデータベース 1 5 5 を更新する。

【 0 0 8 7 】

本実施の形態の暗号入出力処理の手順は、第 1 の実施の形態と同様である。本実施の形態では、暗号エンジン 1 0 3 とコントローラ 1 0 1 との間の通信がインターネット 2 0 を介して行われるので、同一装置内で通信が行われる第 1 の実施の形態に比べてよりデータの漏洩の危険性が増すが、図 8 から図 1 1 で説明したように、暗号エンジン 1 0 3 とコントローラ 1 0 1 との間でも必ずデータを暗号化して送受信を行うので、高い耐タンパ性を実現することができる。

【 0 0 8 8 】

図 2 2 は、電源投入後、ストレージデバイス 2 0 0 にライセンスデータを記憶するまでの一連の A T A インタフェース上の手順を示すシーケンス図である。図 1 2 のイニシャル手順と、図 1 3 のシーケンス I D の確保、図 8 および図 9 のスト

レージデバイス 200 にライセンスデータを記録する手順、図 14 のシーケンス ID の開放までの一連の処理が正常に推移した場合の例である。

【0089】

「Host ATA-IF」は、記録装置 100 のストレージインタフェース 102 に、「Storage ATA-IF」は、ストレージデバイス 200 のストレージインタフェース 202 に相当する。2 つの ATA-IF に挟まれた中央部分には、セキュアコマンドが記載されている。コマンド名の後ろに記載されている (W)、(R)、(S) はコマンドの特性を示すもので、(W) はデータ列の入力を伴うコマンド、すなわち、命令受理後ストレージデバイス 200 からデータ要求があるコマンドであることを示し、(R) は、逆にデータ列の出力を伴うコマンド、(S) は、データ列の入出力を伴わないコマンドであることを示す。

【0090】

また、コマンド「IDENTIFY_DEVICE」、「GET_SECURITY_FEATURE」、「START_SEQUENCE」、「GET_CERTIFICATE」、「PUT_CHALLENGE_KEY」、「CREATE_SESSION_KEY」、「GET_SESSION_KEY」、「PUT_LICENSE」、「WRITE_LICENSE」、「END_SEQUENCE」は、それぞれデバイス情報出力命令、セキュア情報出力命令、シーケンス確保命令、証明書出力命令、チャレンジ鍵入力命令、セッション鍵準備命令、チャレンジ鍵出力命令、ライセンス入力命令、ライセンス書込命令、シーケンス開放命令に相当する。

【0091】

シーケンスは、ストレージデバイス 200 の情報を所得する「Initialization_STEP (イニシャル手順)」と、シーケンス ID を確保する「Start_STEP」、ストレージデバイス 200 の証明書検証からチャレンジ鍵 Ks1 の共有までの「Authentication_STEP」、ライセンスを転送して書き込むまでの「Transmission_STEP」、シーケンス ID を開放する「End_STEP」に区分される。そして、「

WRITE__LICENSE（ライセンス書込命令）」終了後、ライセンスデータを続けてストレージデバイス200に記憶するする場合、「Transmission__STEP」を繰り返しても良い。この場合、安全性は損なわれない。また、「Authentication__STEP」から開始しても良い。

【0092】

以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0093】

実施の形態では、暗号エンジン内において暗号化や復号を行う機能ブロックを別に示したが、それらの構成要素において回路を共有してもよい。これにより、ハードウェア規模を抑え、小型化、低消費電力化に寄与することができる。

【0094】

【発明の効果】

本発明によれば、記録装置とホスト装置との間で秘匿すべきデータを入出力するときの耐タンパ性を向上させることができる。また、本発明によれば、記録装置とホスト装置との間で複数の暗号化入出力処理を並行して実行することができる。

【図面の簡単な説明】

【図1】 第1の実施の形態に係るデータ管理システムの全体構成を示す図である。

【図2】 第1の実施の形態に係る記録装置の内部構成を示す図である。

【図3】 第1の実施の形態に係る再生装置の内部構成を示す図である。

【図4】 第1の実施の形態に係るストレージデバイスの内部構成を示す図である。

【図5】 図2に示した記録装置の暗号エンジンの内部構成を示す図である。

【図6】 図3に示した再生装置の暗号エンジンの内部構成を示す図である。

。

【図 7】 図 4 に示したストレージデバイスの暗号エンジンの内部構成を示す図である。

【図 8】 記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。

【図 9】 記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。

【図 1 0】 再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。

【図 1 1】 再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。

【図 1 2】 ホスト装置とストレージデバイスとの間で並列して処理可能な処理系の数を決定する手順を示す図である。

【図 1 3】 暗号入出力処理の実行に先立って、その暗号入出力処理を識別するためのシークエンス ID を確保する手順を示す図である。

【図 1 4】 暗号入出力処理の実行に先立って、その暗号入出力処理を識別するためのシークエンス ID を確保する手順を示す図である。

【図 1 5】 シークエンス ID を開放する手順を示す図である。

【図 1 6】 ストレージデバイスの暗号エンジンが、ホスト装置が発行したセキュアコマンドを受理する手順を示す図である。

【図 1 7】 ホスト装置からストレージデバイスへ命令が発行される様子を示す図である。

【図 1 8】 第 2 の実施の形態に係るデータ管理システムの全体構成を示す図である。

【図 1 9】 第 2 の実施の形態に係る記録再生装置の内部構成を示す図である。

【図 2 0】 記録再生装置からストレージデバイスへ命令が発行される様子を示す図である。

【図 2 1】 第 3 の実施の形態に係る記録装置の内部構成を示す図である。

【図 22】 第 1 の実施の形態に係る記録装置がストレージデバイスにライセンスデータを記録するまでのシーケンスを示す図である。

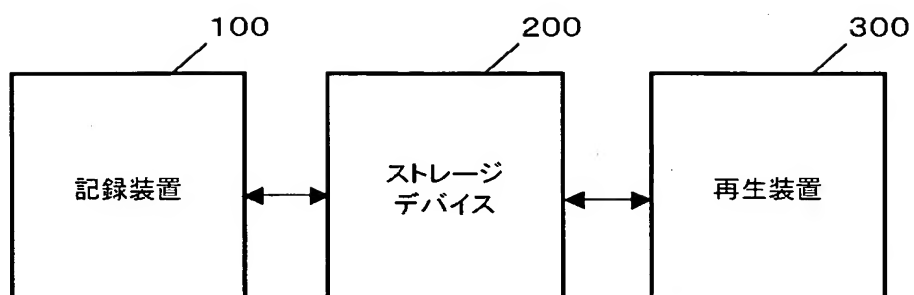
【符号の説明】

10・・・データ管理システム、100・・・記録装置、101・・・コントローラ、103・・・暗号エンジン、104・・・暗号器、105・・・コンテンツエンコーダ、150・・・配信サーバ、160・・・端末装置、200・・・ストレージデバイス、201・・・コントローラ、203・・・暗号エンジン、204・・・通常データ記憶部、205・・・機密データ記憶部、221・・・状態レジスタ、222・・・制御部、223・・・内部レジスタ、300・・・再生装置、301・・・コントローラ、303・・・暗号エンジン、304・・・復号器、305・・・コンテンツデコーダ、400・・・記録再生装置、401・・・コントローラ。

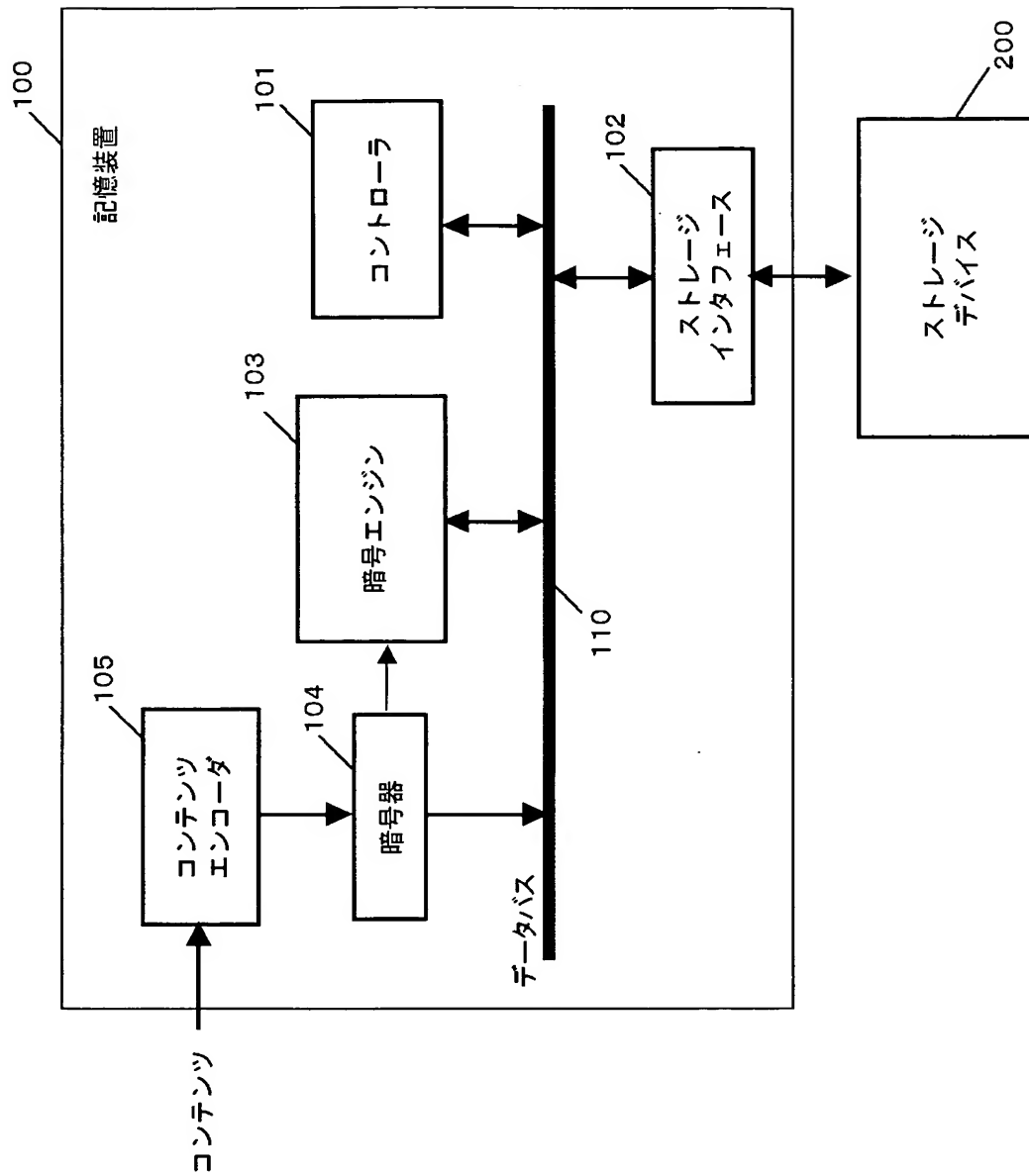
【書類名】 図面

【図 1】

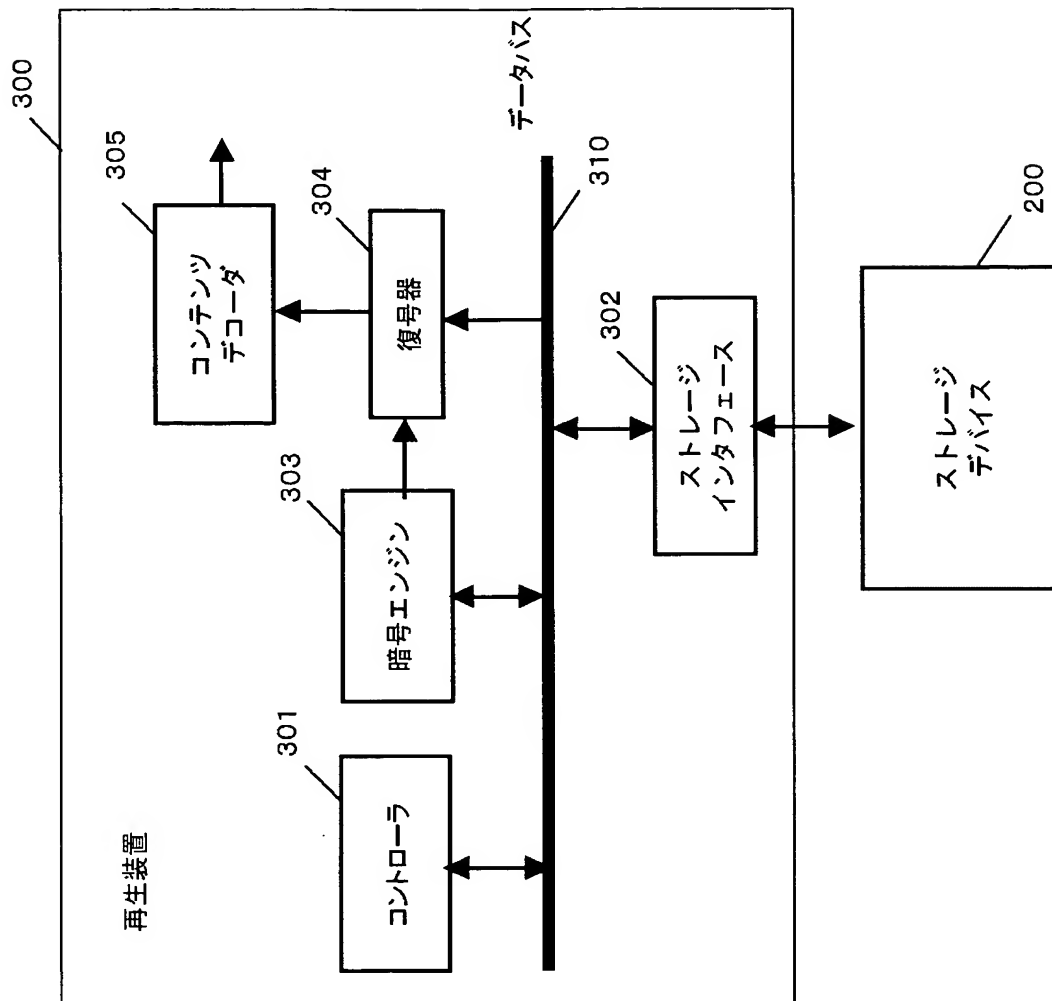
10



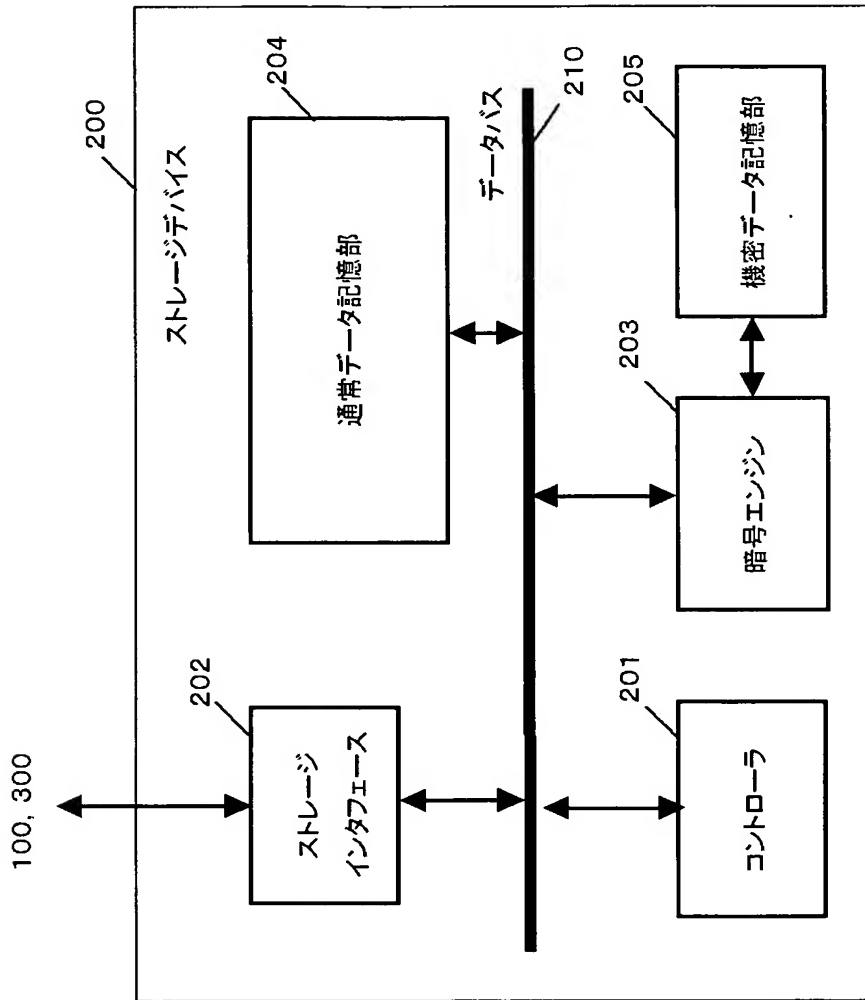
【図 2】



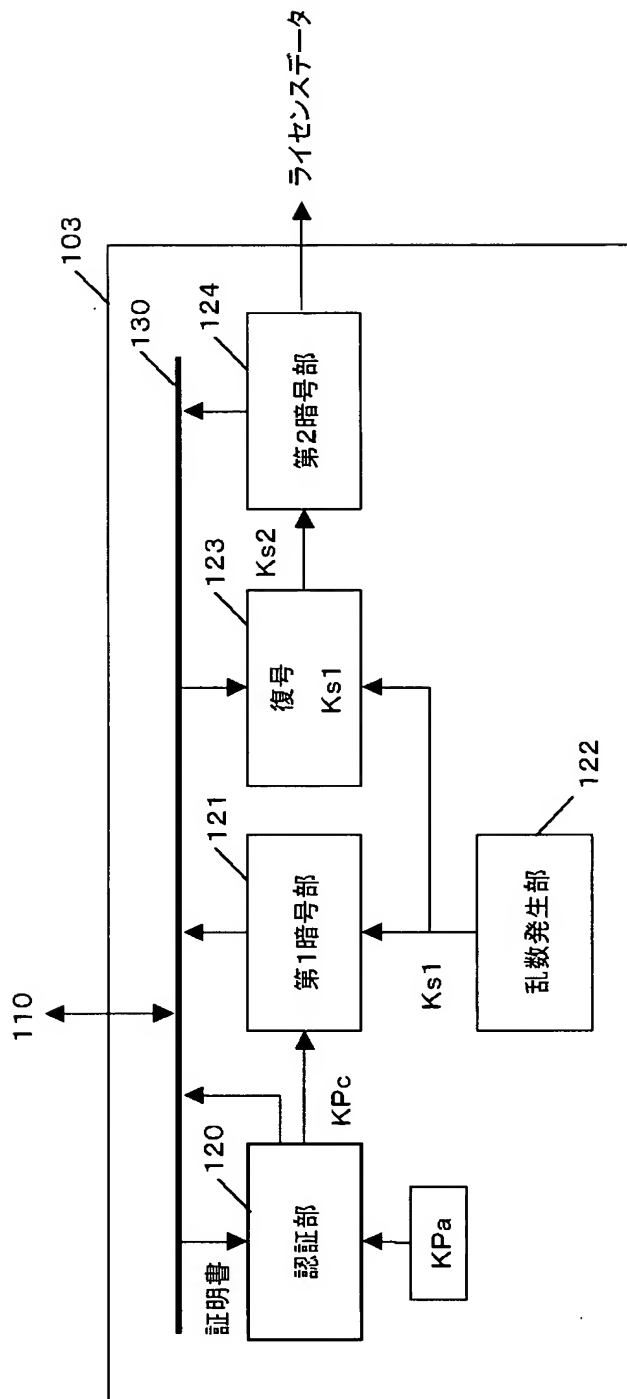
【図 3】



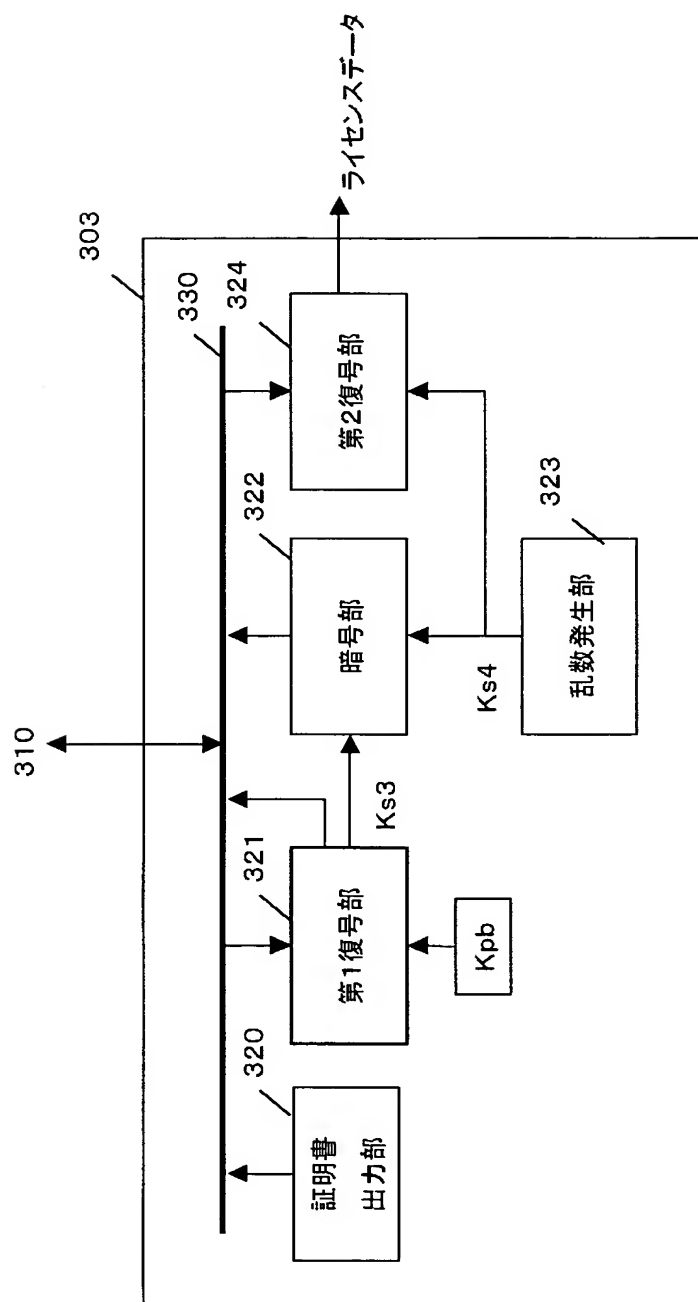
【図 4】



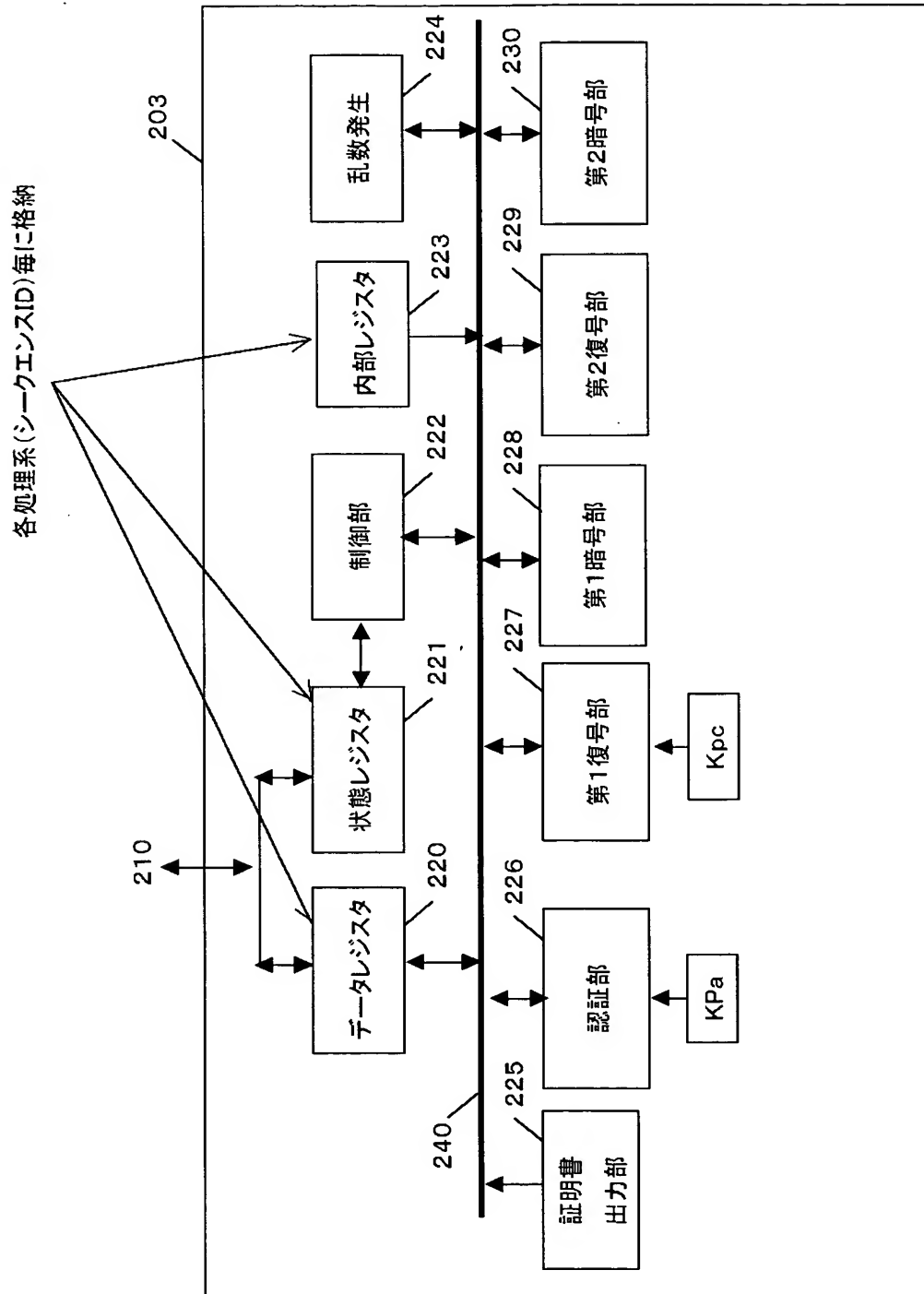
【図 5】



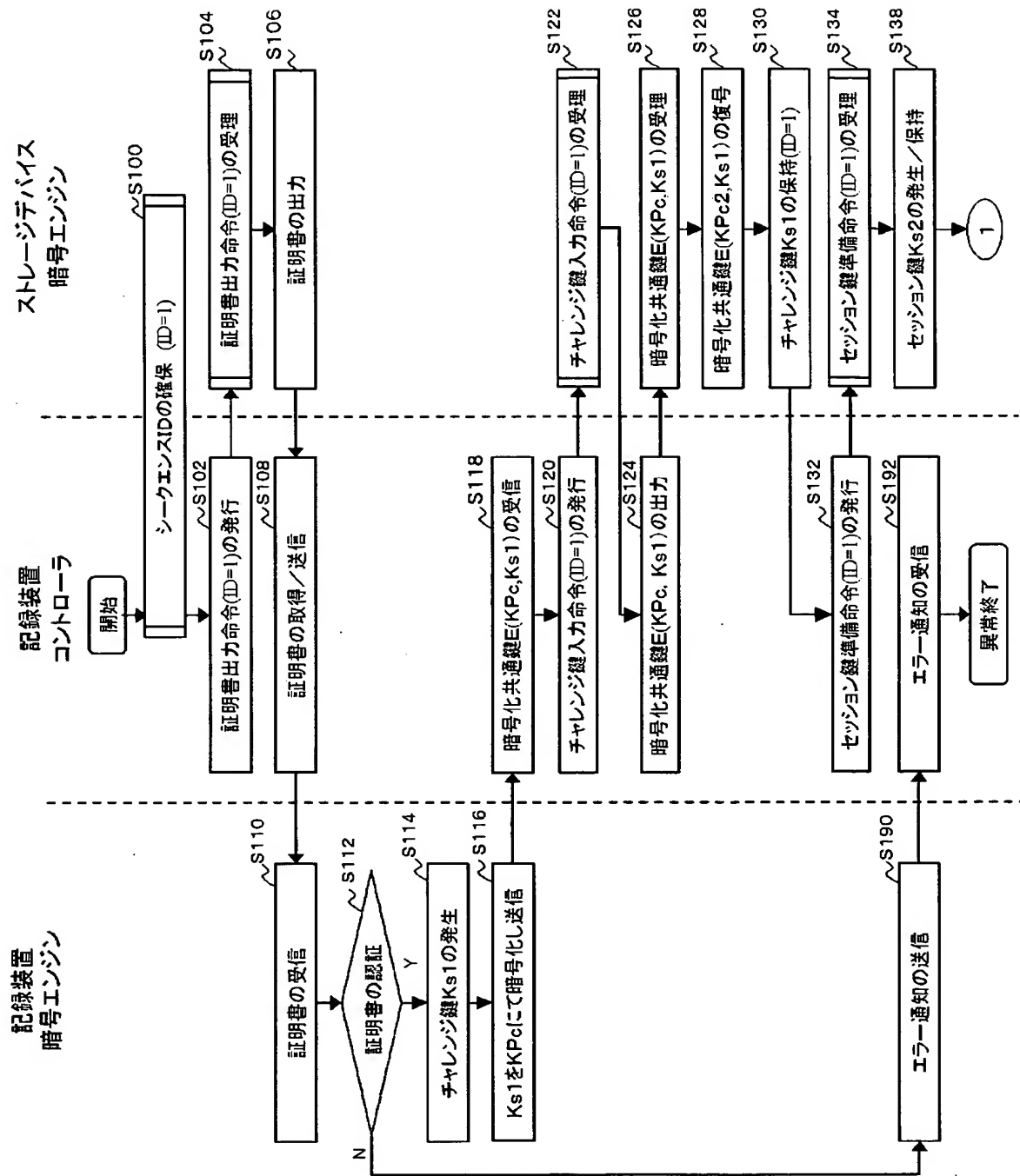
【図 6】



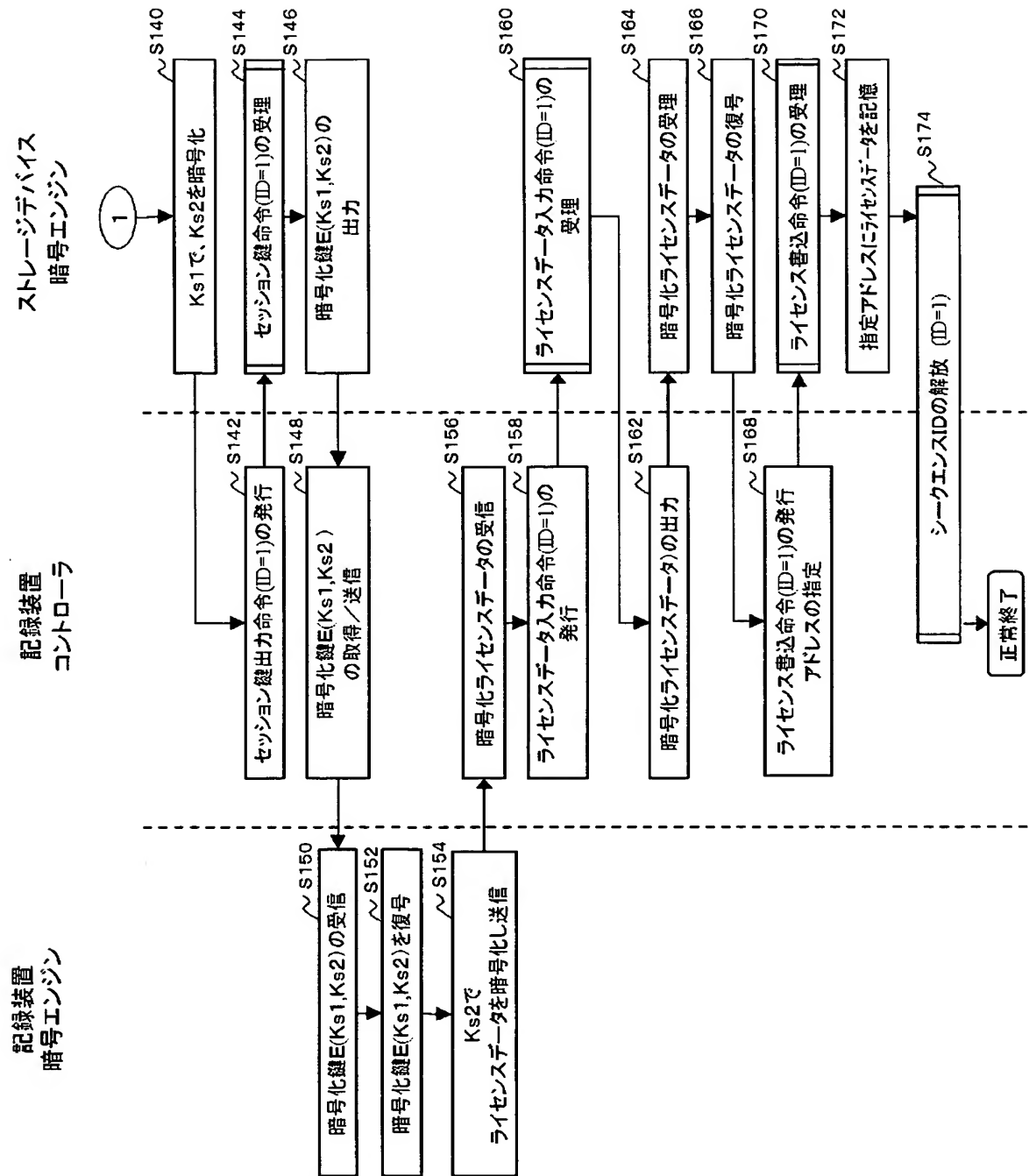
【図 7】



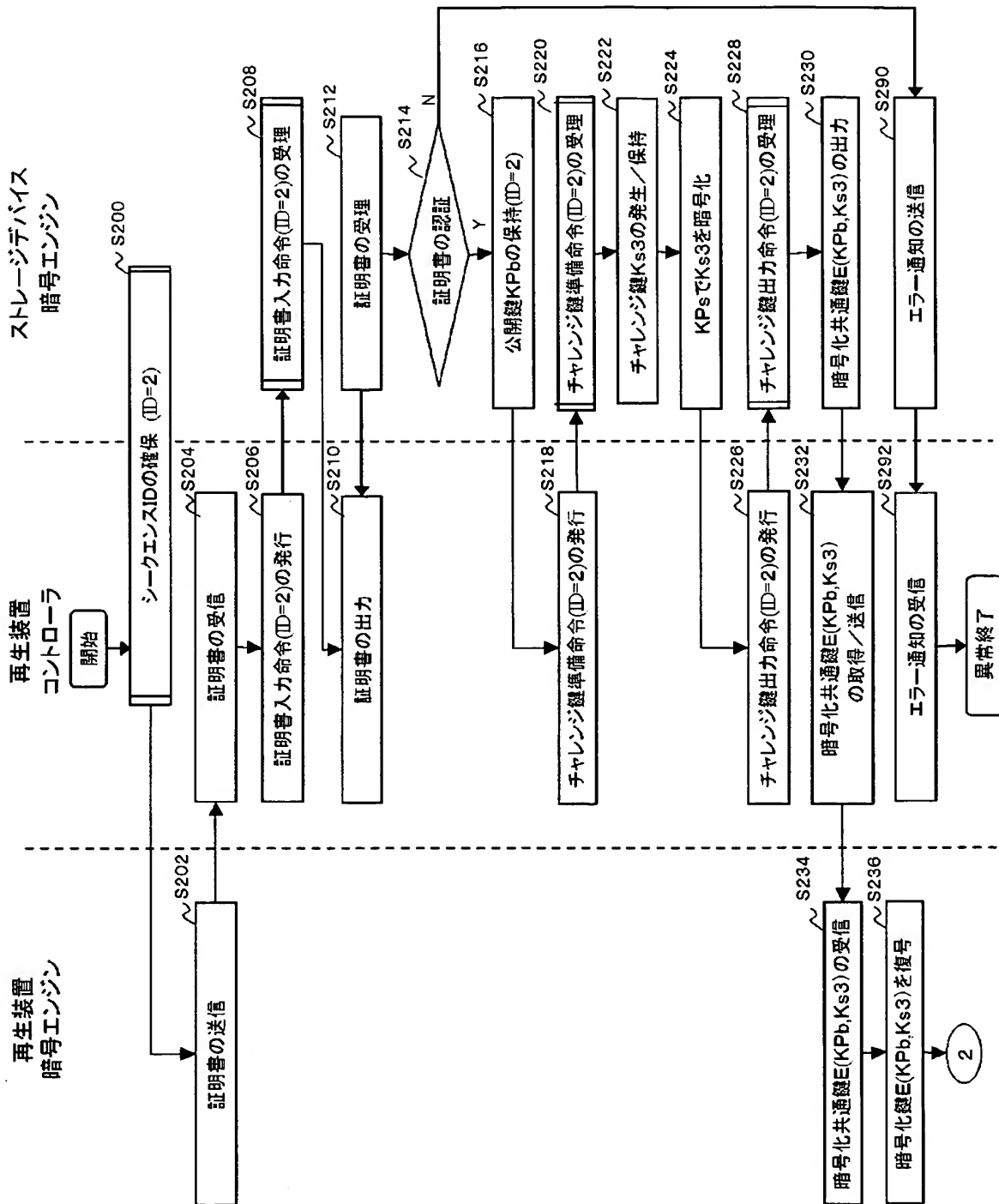
【図 8】



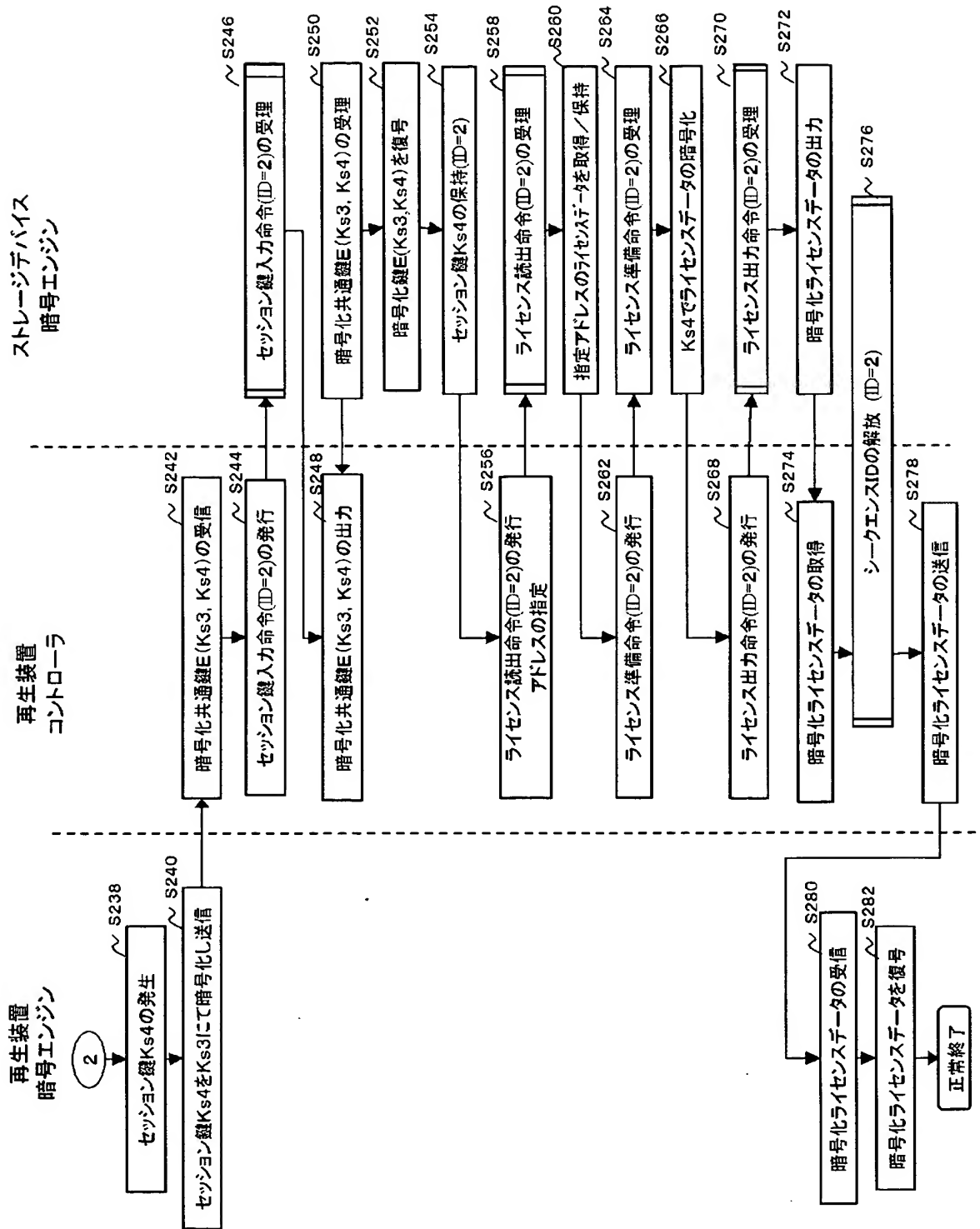
【図 9】



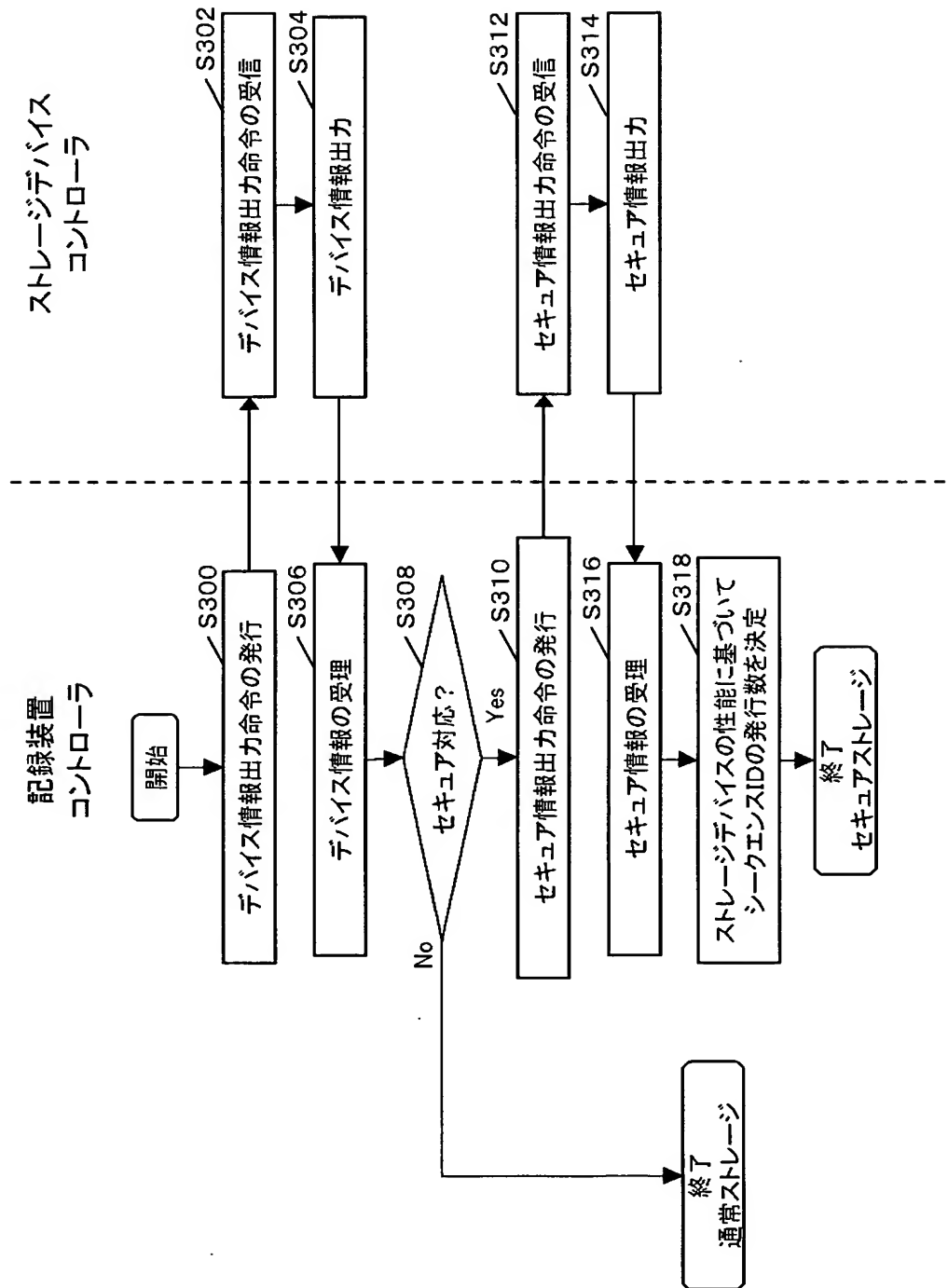
【図 10】



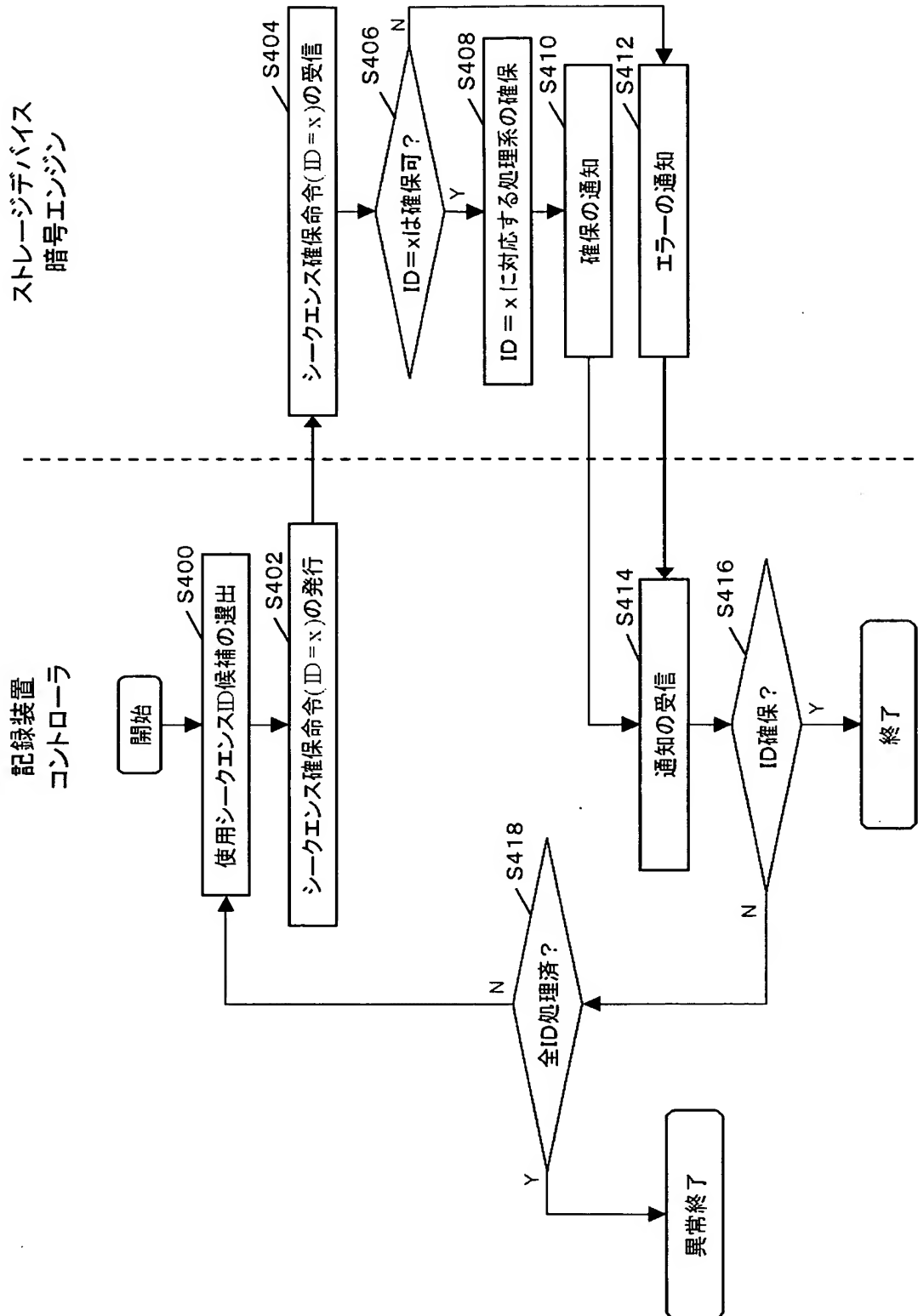
【図 11】



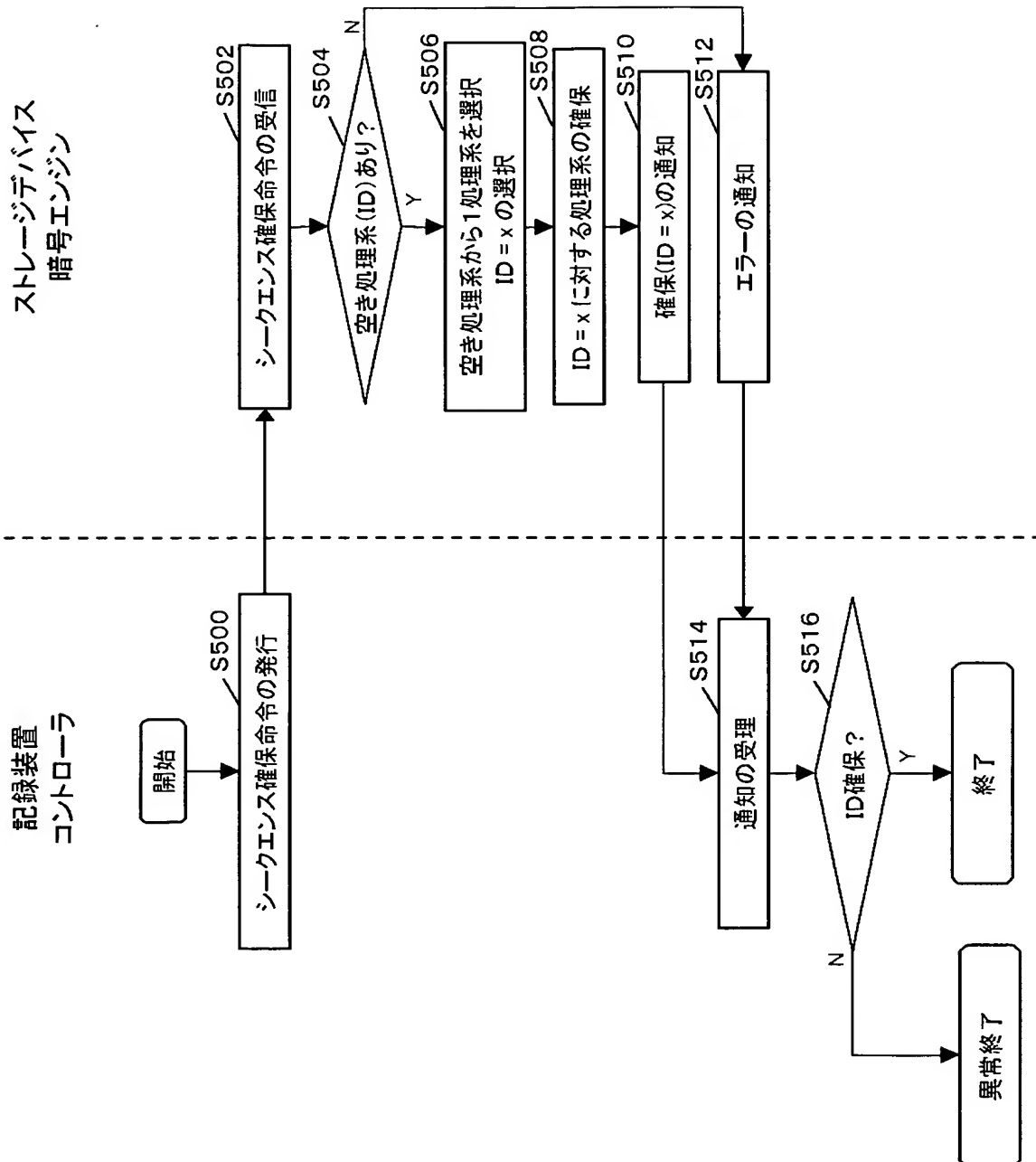
【図 12】



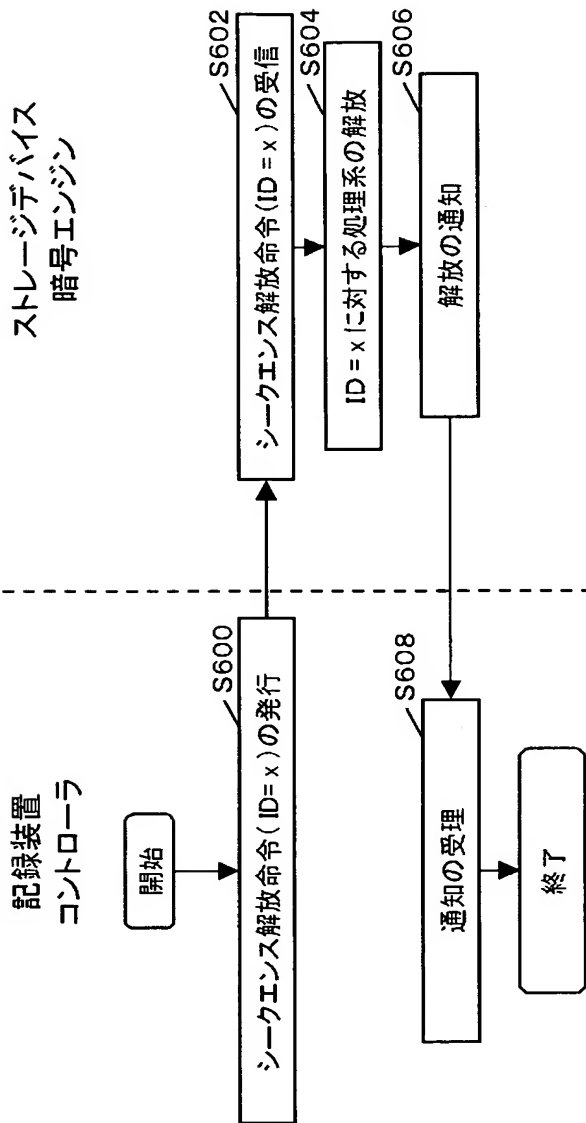
【図 13】



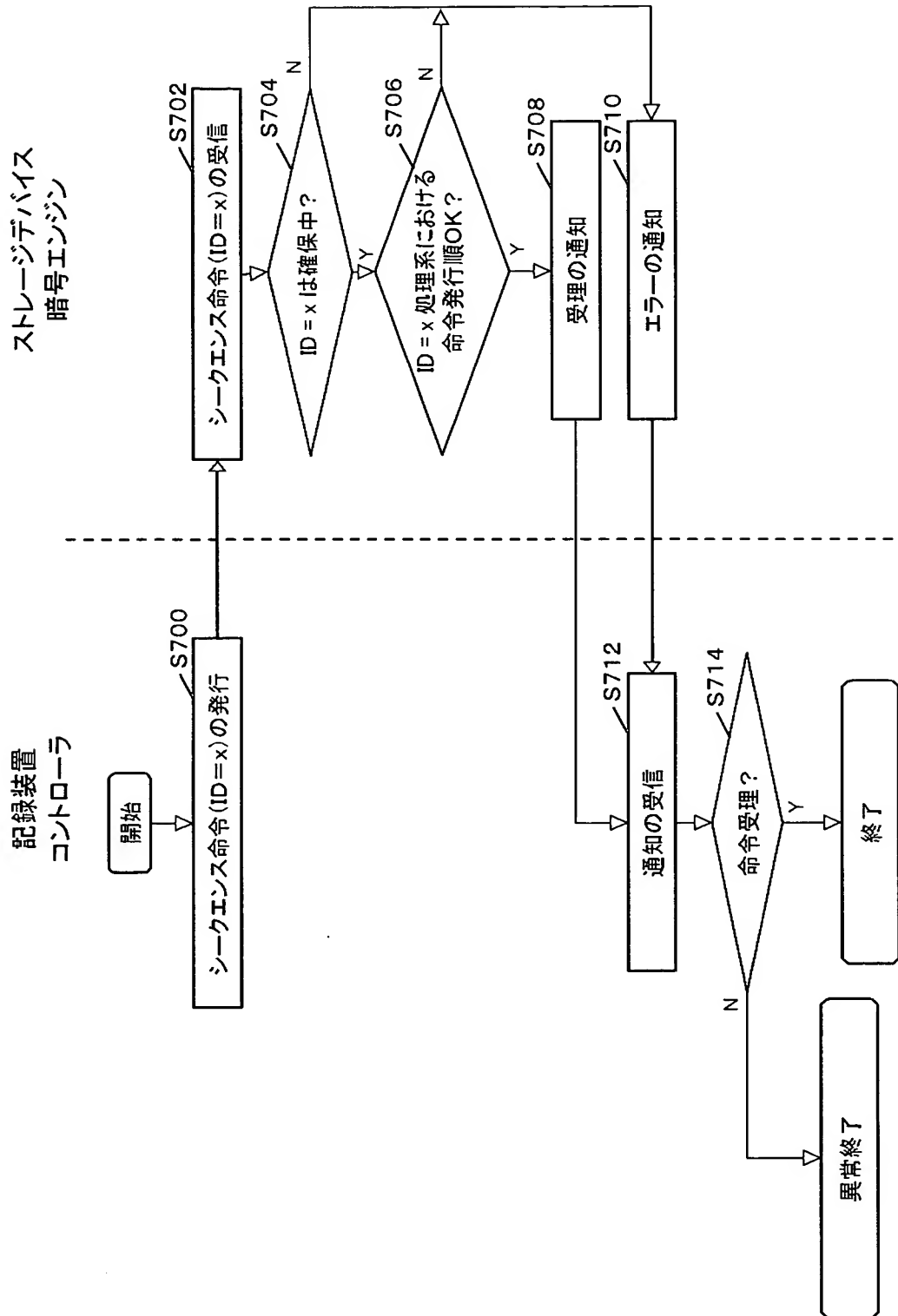
【図 14】



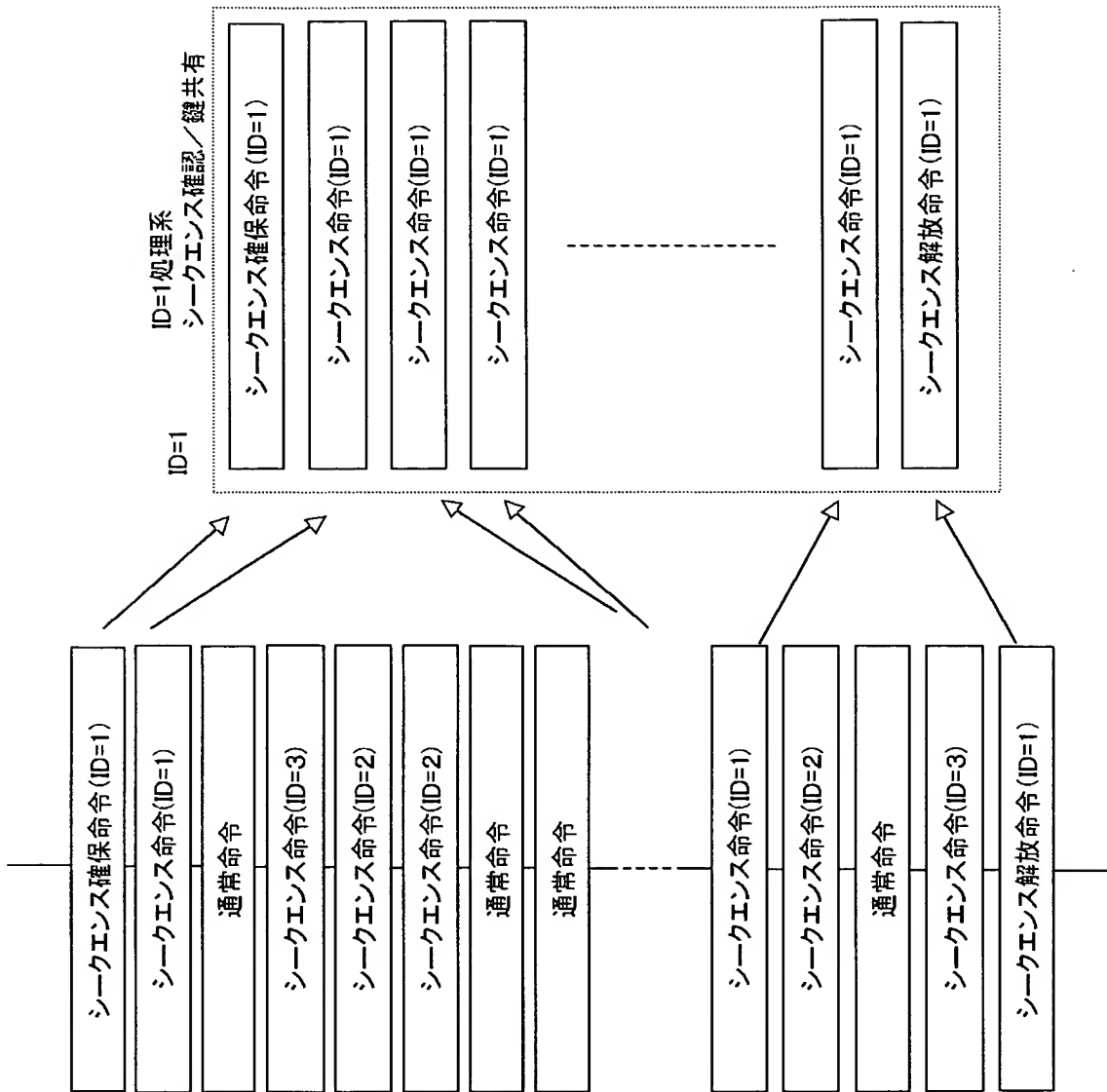
【図 15】



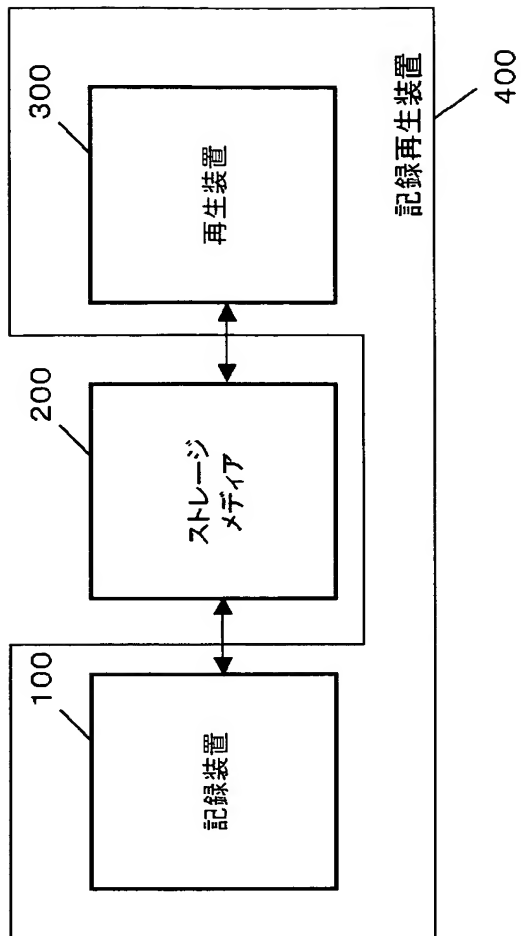
【図 16】



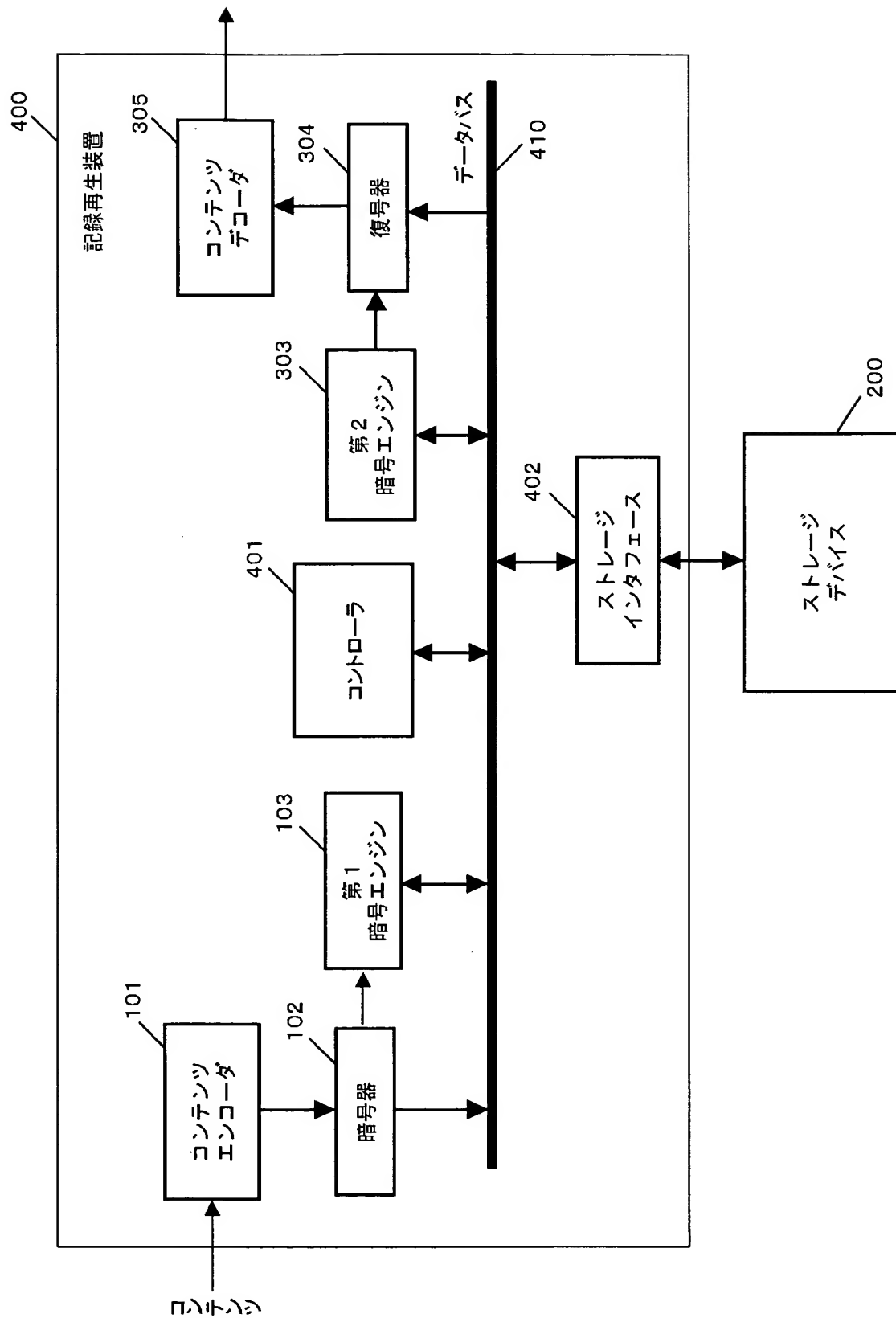
【図 17】



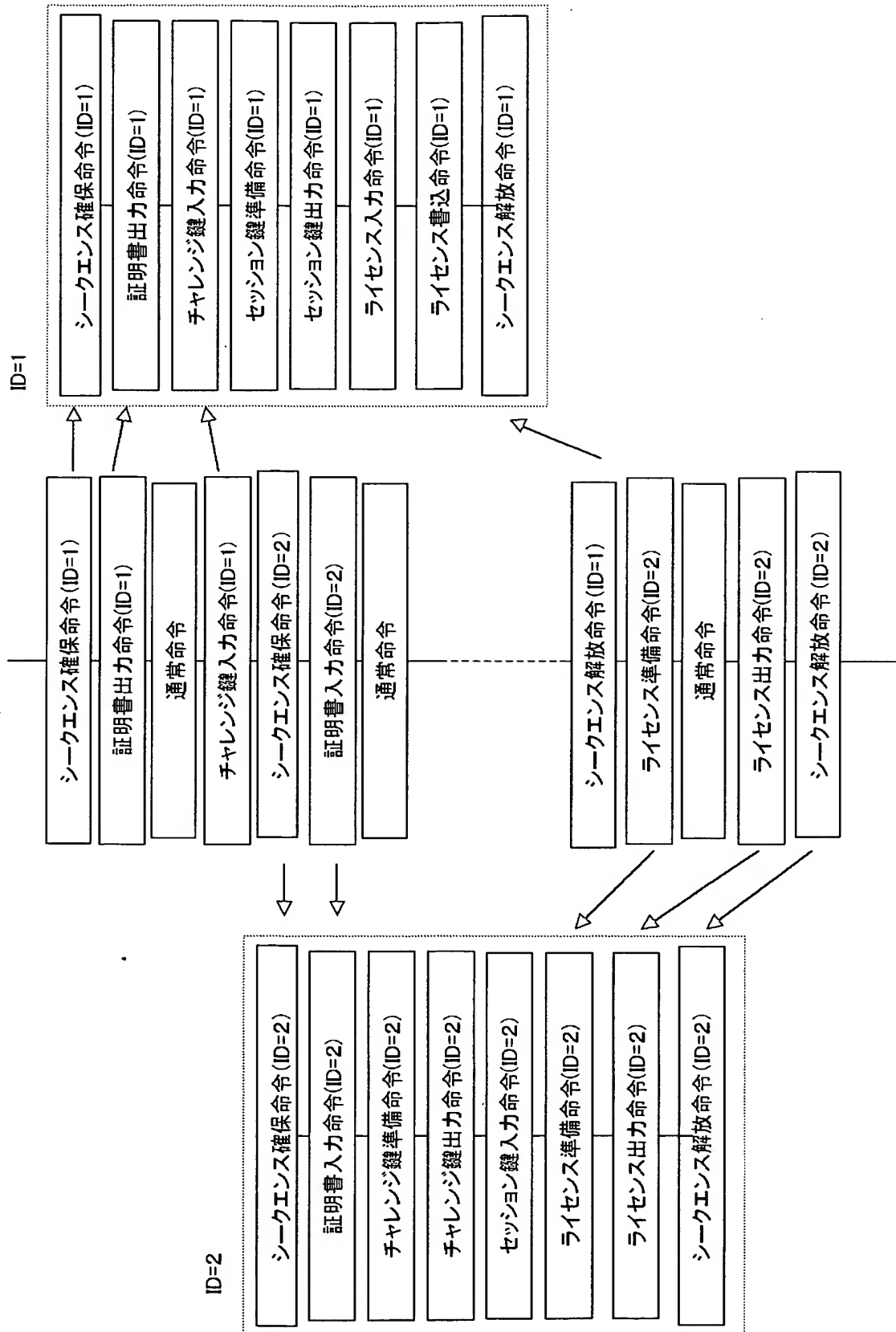
【図 18】



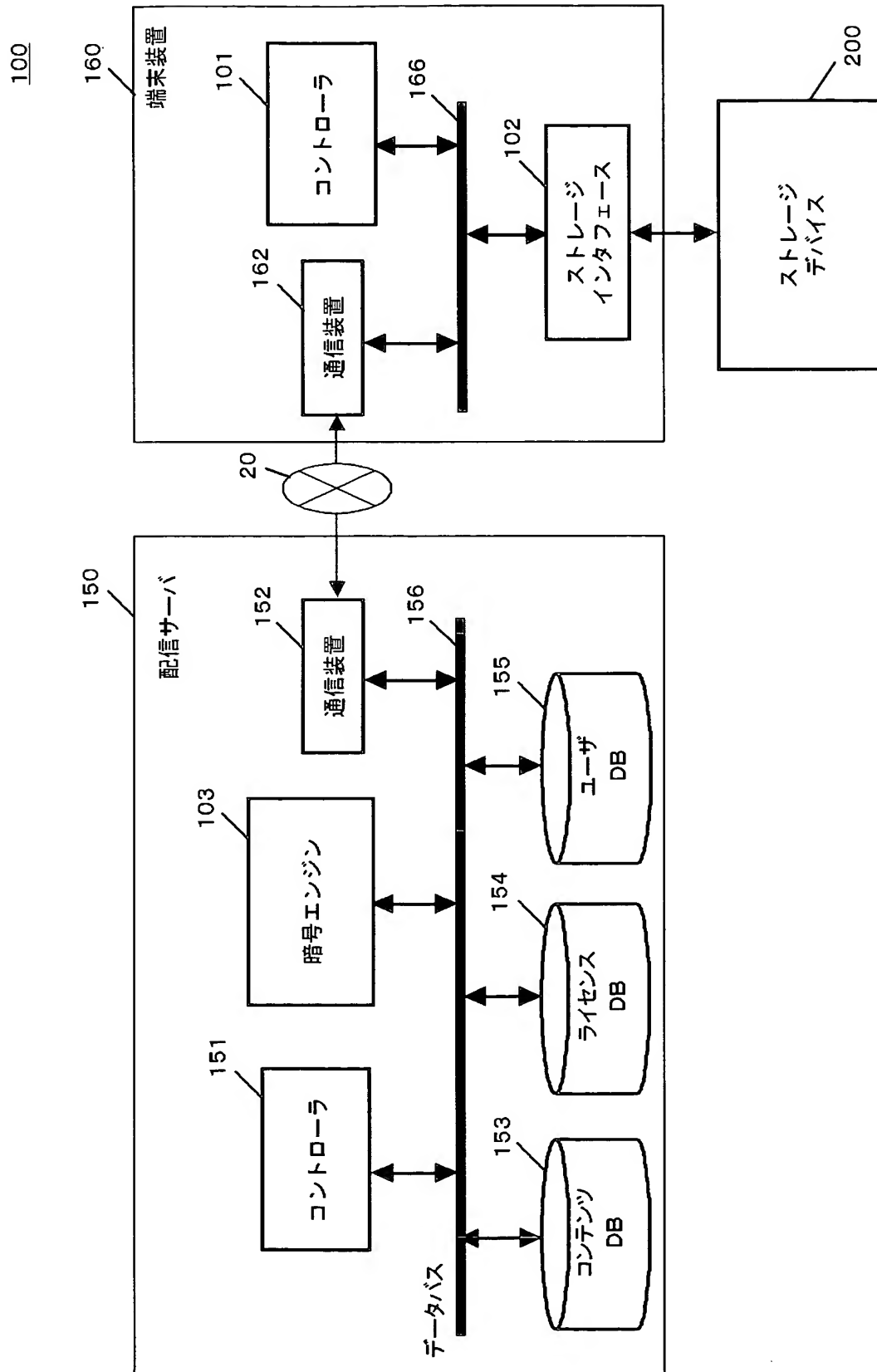
【図 19】



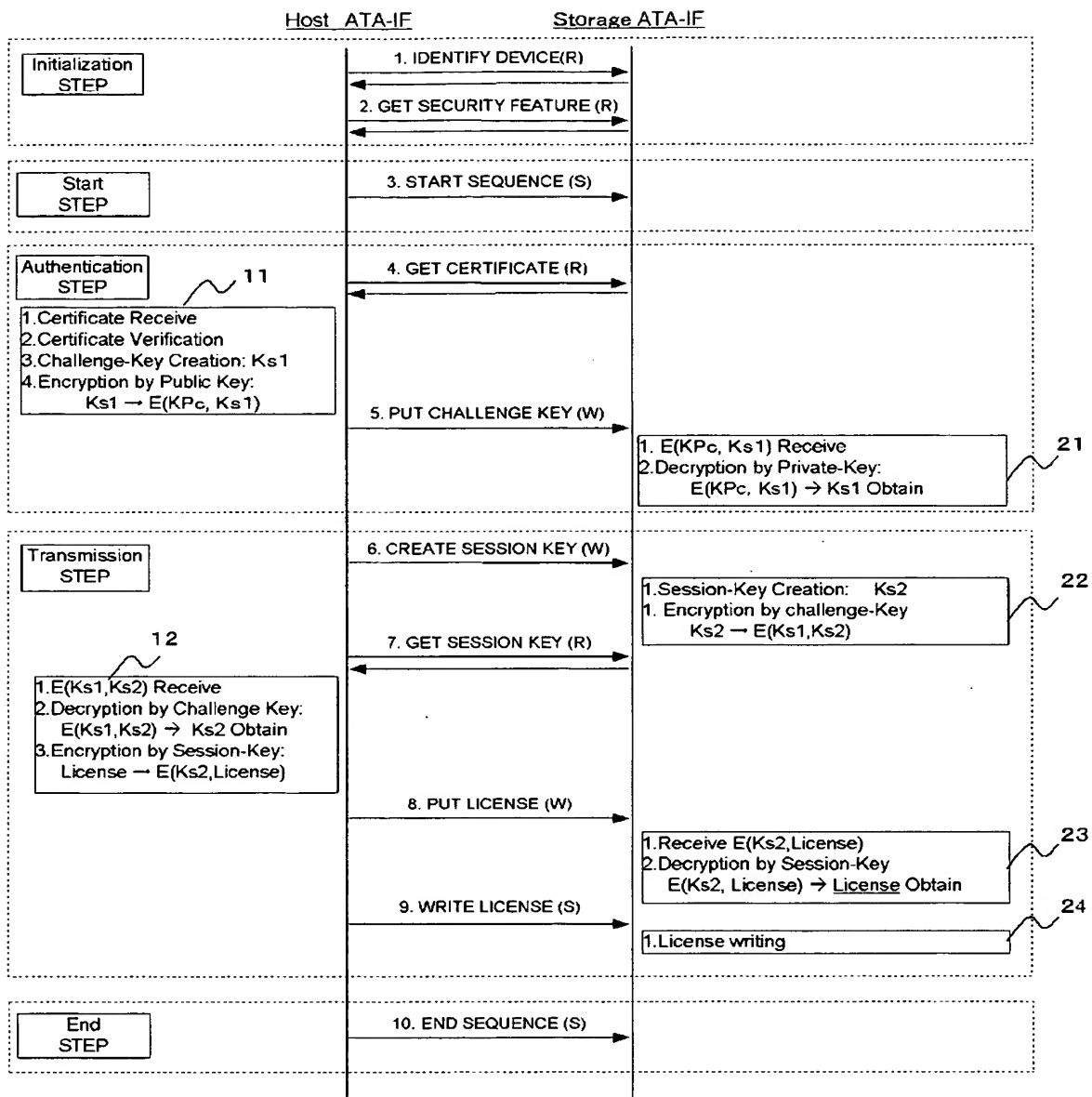
【図 20】



【図 21】



【図 22】



【書類名】 要約書

【要約】

【課題】 記録装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するときの耐タンパ性を向上させる。

【解決手段】 記録装置がストレージデバイスに秘匿すべきデータの入出力命令を発行するとき、その命令がいずれの暗号入出力処理に属する命令であることを識別するための I D を付してストレージデバイスに送る（S 7 0 0）。ストレージデバイスはシークエンス命令を受信すると（S 7 0 2）、その I D が確保されており（S 7 0 4 の Y）、命令発行順が正当であることが確認されると（S 7 0 6 の Y）、その命令を受理する（S 7 0 8）。シークエンス I D により処理系を識別しつつ、命令の実行手順を適切に管理する。

【選択図】 図 1 6

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 1 8 8 9]

1. 変更年月日 1 9 9 3 年 1 0 月 2 0 日

[変更理由] 住所変更

住 所 大阪府守口市京阪本通 2 丁目 5 番 5 号

氏 名 三洋電機株式会社

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 0 4 9]

1. 変更年月日 1 9 9 0 年 8 月 2 9 日

[変更理由] 新規登録

住 所 大阪府大阪市阿倍野区长池町 2 2 番 2 2 号

氏 名 シャープ株式会社

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 3 2 9]

1. 変更年月日 1 9 9 0 年 8 月 8 日

[変更理由] 新規登録

住 所 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地

氏 名 日本ビクター株式会社

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 0 1 6]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都目黒区目黒 1 丁目 4 番 1 号
氏 名	パイオニア株式会社

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号

[3 0 0 0 1 7 6 3 6]

1. 変更年月日

2 0 0 3 年 1 月 8 日

[変更理由]

住所変更

住 所

東京都千代田区丸の内 1 - 3 - 1 東京銀行協会ビル 1 4 F

氏 名

フェニックステクノロジーズ株式会社

特願 2 0 0 3 - 0 9 2 9 4 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社